Scientometrics (2021) 126:2013–2055
https://doi.org/10.1007/s11192-020-03834-6

Towards a systematic description of the field using bibliometric analysis: malware evolution

Sharfah Ratibah Tuan Mat[1] · Mohd Faizal Ab Razak[1] · Mohd Nizam Mohmad Kahar[1] · Juliza Mohamad Arif[1] · Salwana Mohamad[1] · Ahmad Firdaus[1]

Received: 10 April 2020 / Accepted: 9 December 2020 / Published online: 9 February 2021

Abstract
Malware is a blanket term for Trojan, viruses, spyware, worms, and other files that are purposely created to harm computers, mobile devices, or computer networks. Malware commonly steals, encrypts, damages, and causes a mess in these devices. The growth of malware attacks has a consequence on the growth and attractiveness of mobile features in mobile devices. Most malware research aims to probe the different methods of preventing, analysing, and detecting malware attacks. This paper aims to demonstrate an exhaustive knowledge map of the Android malware by collecting a ten (10) year dataset from the Web of Science database. A bibliometric analysis was employed for analysing articles published between 2010 and 2019. Using the keyword "malware", 5622 articles were retrieved. After scrutinising with the keywords of "Android malware", 1278 articles were then collected. This study provides an overview of the articles, productivity, research area, the Web of Science categories, authors, high-cited articles, institutions, and impact journals examining malware. Research activities are continued by placing terms in the classification of malware detection systems that outline important areas in malware research. From the analysis, it can be concluded that the highest number of publications focusing on malware studies came from the continent of Asia. Additionally, this study discusses the challenges of malware studies in the recent research studies as well as the future direction.

✉ Mohd Faizal Ab Razak
faizalrazak@ump.edu.my

Sharfah Ratibah Tuan Mat
sharfah0206@gmail.com

Mohd Nizam Mohmad Kahar
mnizam@ump.edu.my

Juliza Mohamad Arif
juliza.m.arif@gmail.com

Salwana Mohamad
salwanamohamad@ump.edu.my

Ahmad Firdaus
firdausza@ump.edu.my

[1] Faculty of Computing, University Malaysia Pahang, 26300 Gambang, Kuantan, Pahang, Malaysia

Keywords Bibliometric · Android malware · Web of science · Intrusion detection system

Introduction

Malware is a term used for all kinds of malicious software designed to attack and damage a computer system. The common malware causing harm to the network and operating system include Trojan horse, worm, virus, spyware, ransomware and adware (Razak et al. 2016). These malware attack the system in different methods (Qamar et al. 2019). Such a malware is proficient in triggering destruction to the operating system and networks. In Quarter 2 (Q2) of 2019, malware targeting mobile devices had increased by 50% as compared to the previous year (Palmer 2019). In January 2019, a total of two billion hacked records had been uncovered (Sanders 2019). McAfee Labs noted that attacks from ransomware had grown by 118% in 2019 (Mcafee 2019a, b) while banking Trojan had doubled from June to September 2018, serving as the most vigorous in growth, among the malware families (Mcafee 2019a, b). A new malware reported by Chebyshev et al. (2019) revealed that the new Trojan Android.MobOk took money from mobile accounts by using subscriptions. To date, a total of 905,174 malicious installation packages had been detected by Quarter 1 of 2019. The number had decreased by 151,624 in Quarter 2 of 2019. Statistics showed that the risk tool had increased by 41.24% in 2019 as compared to only 30.20% in 2018. Furthermore, the percentage of adware and Trojan was noted to have increased by 18.71% and 11.83%, respectively in 2019. This substantial growth in mobile attacks over the years showed that attackers were progressively noticing that the Android mobile devices are attractive targets (Verkijika 2019).

The Android network offers attractive functions for communication, such as entertainment, data storage, and social communication (Chen and Li 2017). The acceptance of the operating system in Android mobile devices has been one of the most targeted by malware, spurring the attention of unscrupulous authors (Shrivastava and Kumar 2019a). These people have been encouraged by their own unscrupulous goals and other lucrative benefits. The lack of priority given to security by mobile device developers has also caused the exploitation of malware into mobile devices (Thompson et al. 2017). To combat the security issues, Android itself has provided sand-boxing for security mechanism; however, malware authors creatively manipulated other vulnerabilities of Android to spread the malware (Qamar et al. 2019). In addition, the lack of user awareness (Lopes et al. 2019), and the vulnerabilities of a computer operating system boost the opportunity for malware to exploit data through malicious codes (Goel and Jain 2018). These malicious programmes accomplish different purposes, such as encrypting, stealing crucial information stored in phone storage, removing important data, modifying or controlling main computing functions, and capturing the activities that are unknown to the users (Basu et al. 2019). The reliance on mobile devices by most users for their personal work through Wi-Fi access (Sharma and Gupta 2018a) gives feasibility to attackers to attack a user's credential (Sharma and Gupta 2016). The awareness on the emerging of malware should be alerted to all mobile users as a way to prevent the devices from being damaged.

To prevent the dissemination of malware, devices are protected by using existing methods such as anti-malware software and the intrusion detection system (IDS) (Talal et al. 2019). Nevertheless, novel approaches are still needed to detect the rapid increase in malware attacks throughout the year. With the advent of more advanced technologies, malware authors are able to hide malware from detection. Malware authors applied a diverse

sophisticated obfuscation technique including encryption, packing, polymorphism and metamorphism (Huda et al. 2018). It is generally used to prevent signature extraction originating from the malware's binary code (Or-Meir et al. 2019). This phenomenon has prompted many researchers to investigate and analyse the features of malware. Most of the studies were conducted so as to introduce a better approach of preventing, detecting, and proposing a new approach to solve Android malware. A study by De Lorenzo et al. (2020) used dynamic analysis with Vizmal to spot and avoid malware. Vizmal is a visualisation tool used to trace the execution of applications in Android. It is used to overcome the issue of obfuscation created by malware authors. Rolling acts as an assistant during inspection of malware analysis and observes the localisation of malicious. Others studies such as Yerima et al. (2014) and Yu et al. (2013) applied the Bayesian technique to detect malware. Another study Magdum (2015) used a feature of permission-based dimension in machine learning to identify the malware. All these studies which described the research activities in this field are crucial. Despite the many research activities that have been published, the bibliometric study of malware likewise becomes popular in today's research trends to provide an impactful study.

Bibliometric is a quantitative analysis of articles published in a specific field (Blanco-Mesa et al. 2017; Baker et al. 2019). The bibliometric study analyses the data and features of articles, such as productivity, research area, Web of Science (WoS) categories, authors, high cited articles, institutions, and impact journals. The bibliometric method is used to evaluate the impact of published articles and to assist the researcher in understanding the structure of the research life (Reuters 2008). It reveals the area of the studies, thereby increasing the interest and attention of researchers and funding institutions. Analysis derived from the bibliometric method is able to compare the countries that contributed to the publications according to their respective fields. Bibliometric study has been applied in a wide range of fields including the COVID-19 pandemic (Gautam et al. 2020), environmental (Zhang et al. 2020), agricultural (Luo et al. 2020), sustainable development (Ye et al. 2020), Chinese loess plateau (Zhang and Chen 2020), accounting (Merigó and Yang 2017), economic (Bonilla et al. 2015), linguistic decision making (Yu et al. 2016) and fuzzy research (Merigó et al. 2015). Bibliometric studies contribute to several advantages such as: (a) reveal the importance of research in the related field, (b) reveal the development of research based on the institution and performance, (c) enable researchers to use the publication of related studies for future studies, and (d) to improve the knowledge of new researchers.

The current study aims to evaluate studies done on the Android malware which have been published in the WoS from the year 2010 to 2019. The study scrutinises the Android malware research topic, publication pattern, research area, authors, highly cited articles, impact journals, and the institution of the studies. The significant aspect in this analysis is that the Web of Science has a wider view of the contributions. In planning the review of Android malware articles in the WoS database, the following steps were followed: (1) identify and analyse the Android malware study in the Web of Science for 10 years (2009–2019); (2) present the findings of Android malware detection considering articles, productivity, research area, the Web of Science categories, authors, high-cited articles, institutions, and impact journals; (3) define and study the research gap, the highlighted questions, and the difficulties encountered in the prior studies; and (4) identify the latest trends on Android malware attack. The objective of classifying these steps is to deliver a better understanding of Android malware. The proliferation of Android malware studies has been analysed to determine the tendency of malware pattern and the detection procedures taken to prevent the spreading of malware. Focusing on the past 10 years publication

of malware specifically for Android malware study, this bibliometric analysis similarly looked at the introduction of the scope and aims of the study by planning and evaluating the challenges in malware trends.

The current study used "android malware" as the main keyword to get the related publications. The keyword is imperative in order to retrieve current information on the research trend, and also to disclose the research direction and attraction. The related publications were searched by using the WoS Core Collection database. Limit was set at the past 10 years (2010–2019). Additionally, this paper also discussed the malware detection system and the challenges in malware study. As a summary of the paper, we analysed the research publication comprising seven (7) continents including Asia, Europe, North America, the Middle East, Australia, South America, and Africa. Asia had the highest publication at 40.5%, among all the continents, followed by Europe with 26.5%, and North America with 20.3%. This showed that Asia outperformed Europe by a difference of 14% while North America and Europe had some disparity. The continent with the least contribution of publication of Android malware seemed to be Africa, at 0.7% only. Table 1 illustrates the distribution of the publication in seven continents.

The remainder of this paper is systematised as follows. Section 2 discusses the process of collecting data. Section 3 provides the findings of the studies. Section 4 explains the taxonomy for the detection system of malware. Section 5 discusses the challenges and imminent trends and Sect. 6 concludes the paper.

Methodology

Bibliometric is defined as the statistical method used to analyse articles, books, and other publications. It is frequently used in the library and information science field (Library 2020). Bibliometric is similarly referred to as scientometrics. Bibliometric analysis covers part of the research evaluation methodology, and various kinds of literature tend to have their own method of bibliometric analysis (Ellegaard and Wallin 2015). According to Razak et al. (2016), bibliometric is a process to appraise, analyse, and envision the arrangement of scientific fields. The bibliometric approach focuses on quantitative analysis, such as citation counts. In such analysis, the term 'complementary' is used as a qualitative indicator to search for issues like funding granted, rewards received, peer review, and number of patents (Library 2019). The key concepts of the bibliometric approach are output and impact, which are used as a measurement for publications and citations. Hence,

Table 1 Publication of 7 continents

Continent	Publication %
Asia	40.5
Europe	26.5
North America	20.3
Middle East	8.7
Australia	2.3
South America	1.0
Africa	0.7

bibliometric studies give many advantages in order to provide the important trend of the research topic.

Bibliometric analysis has been used in various areas of study. The bibliometric study done by Shanker et al. (2020) analysed the studies of neurosurgeon's academic works in the New York metropolitan area. Another bibliometric study was by Iwami et al. (2019) who examined fields that co-evolved with information technology while (Ospina-Mateus et al. 2019) analysed the study of motorcycle accidents. A study by Baker et al. (2019) in the field of financial economics used bibliometric analysis to present the productivity and impact of RFE (review of financial economics). Additionally, Prashar and Sunder (2019) used bibliometric study in the field of sustainability development, Raparelli and Bajocco (2019) in the field of vehicle agricultural and Galetsi and Katsaliaki (2019) in the field of Information Science. Comparatively, the bibliometric study of malware is only just emerging in research trends as compared to other fields. In this study, the researcher illustrates how to evaluate the research by using the bibliometric method. The evaluation is conducted through the analysis to get the impact of the articles. Table 2 analyses past studies which had applied the bibliometric approach, in which the current study is similarly applying. However, there are some dissimilarities noted on the keyword and findings used.

For the development of this study, the author used the database Web of Science which belongs to Thomson Reuters. In this study, WoS core collection database was chosen and SciELO Citation Index, KCI-Korean Journal Database, and Russian Science Citation Index were removed. The selected articles are solely written in English. To carry out the research analysis, the keywords malware and android malware were used to distinguish the numbers of publications of both keywords. The keyword Android malware focused on the publication of mobile malware while the keyword malware generated global information of malware including cybercrime, IoT, phishing and many more articles of malware in the WoS. The advantages of using the keyword 'Android malware' is the collected articles are related to mobile malware and resulted in better in findings. Thus, the Android malware is selected for the keyword in this bibliometric study.

The data for this study were analysed two times by considering the changes of number of the publication in the WoS database. Firstly, analysis of data was on October 2019 and secondly in February 2020. In February 2020, there were 1278 articles of Android malware and 5622 articles for malware. In this filter, 97 articles were excluded consisting of the SciELO Citation Index, KCI-Korean Journal Database, and Russian Science Citation Index. Then, the selected 1278 articles were analysed for the title, year of publications,

Table 2 The list of studies of bibliometric methods

References	Fields	Year
Prashar and Sunder (2019)	Sustainability development	2020
Shukla et al. (2020)	Medical Informatics	2020
Galetsi and Katsaliaki (2019)	Information Science	2019
Baker et al. (2019)	Financial economics	2019
Lu et al. (2019)	Public health	2019
Ahmad et al. (2019)	Dental traumatology	2019
Raparelli and Bajocco (2019)	Vehicle agricultural	2019
Firdaus et al. (2019)	Blockchain	2019
Razak et al. (2016)	Malware	2016
This study	Android malware	2020

research area, author/s, citation, institution/s and impact journal. These articles included articles, journals and book chapters. With the selected 1278 articles, an analysis was done by forming the affiliation between the research area, author/s, citation, institution/s and impact journal. Finally, the open-source application called R was used as a tool to visualise the final result. R was used because this tool supports many bibliographic visual for analysis and comprises excellent features. Figure 1 clarifies the data collection process.

Web of Science (WoS)

The Web of Science (WoS) is a webpage that offers multiple databases for indexed journal articles. Formerly known as the Web of Knowledge, the WoS was introduced by the Institute for Science Information (ISI). It is presently managed by Clarivate Analytics (Iwami et al. 2019). The WoS has indexed coverage starting from the year 1900. The WoS has covered more than 12,000 impact journals, with 148,000 journals and book-based proceedings, across 256 disciplines in science, social sciences, and humanities (Webofknowledge 2018). It provides the basic search, cited reference search, author search, and advanced search, from four databases such as the Web of Science Core Collection, the KCI-Korean Journal Database, Russian Science Citation Index, and SciELO Citation Index. The WoS provides the citation report; it also analyses the result so that it can track the activities, and the impact of the journal through an appropriate keyword search.

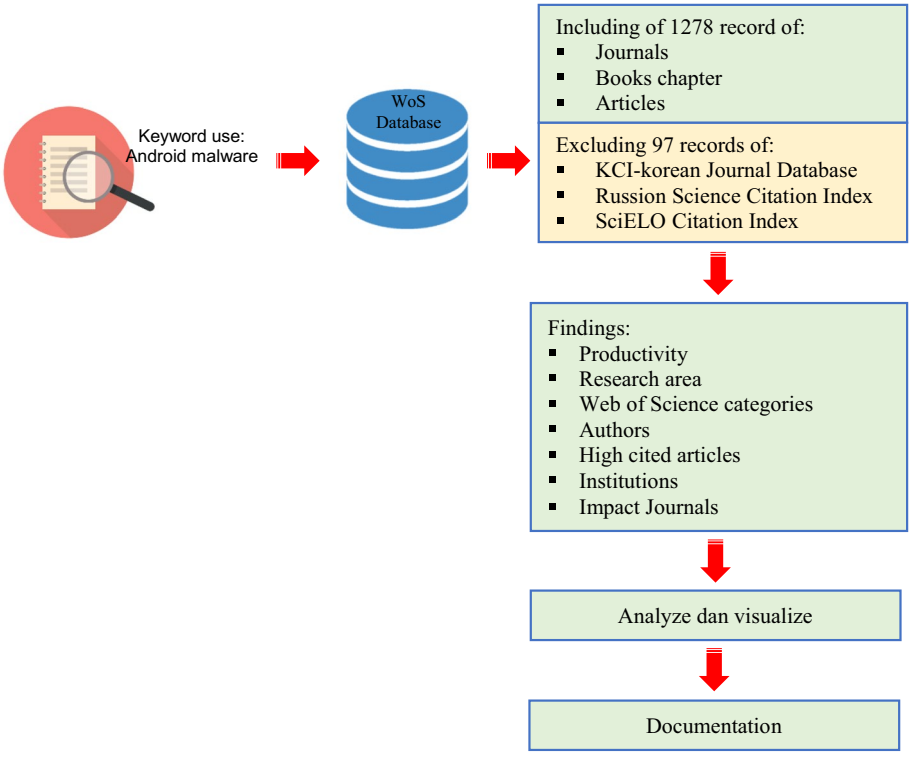


Fig. 1 Methodology of data collection

This study chose the WoS database because the contents of the WoS had been evaluated before, based on publication impact, review, influence, and geographical distribution. The WoS served as a research tool that accommodates the user in acquiring the information, and in analysing and disseminating knowledge. The WoS has innumerable capabilities of search and analysis. These are useful for researchers when searching for index journals in their respective areas. The indexing was first used to search for the results across disciplines. Past studies of bibliometric included Baker et al. (2019), Shukla et al. (2020), Yao et al. (2020) and Chen et al. (2019) which utilised the WoS database comprising of science, social science, arts, and humanities field. Besides the WoS, there are other database websites, such as ScienceDirect, Elsevier's Scopus, IEEE Explore, Google Scholar, and Springer.

Findings

This section describes the findings of Android malware studies. Articles between 2010 and 2019 were analysed. Findings were divided into seven (7) sub-topics: publication year, countries, research areas, authors, institutions, highly cited article, and impact journals. The total publications were noted to be 1278 articles, as presented in Table 3.

The statistics in Table 3 showed that publications of Android malware studies had increased twice in amount, starting from 2011 until 2014. The highest publication was in 2017, with 254 publications. The increased publication can be attributed to the wild growth of malicious software on Android devices. This seemed to have encouraged researchers to examine the factors infected by malware, the vulnerabilities of the devices, and the impact and method used to prevent and reduce those malware attacks. Publications on Android malware dropped slightly in the year between 2018 and 2019. The reason can be attributed to the delayed time taken by reviewers and publishers to accept such articles. Figure 2 describes the type of publications based on the years.

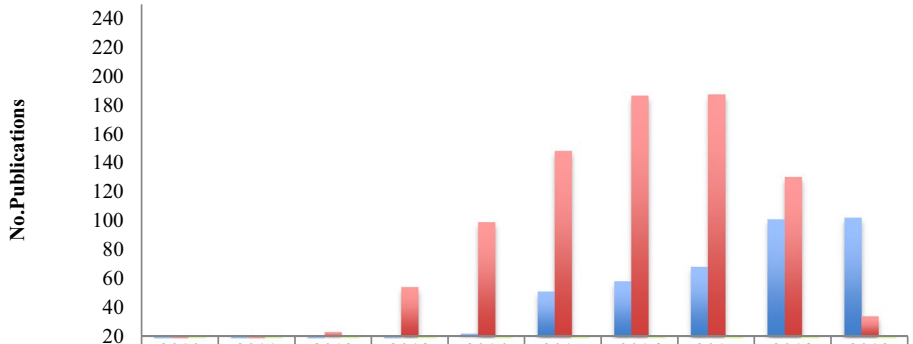
In Fig. 2, it is noted that publications were increasing smoothly year by year. This occurrence then dropped slightly in 2018, and more significantly in 2019. Undoubtedly, publications of journals consume time from acceptance of articles to publication, hence the rate in publication showed a decline. This had clearly affected the number of publications for that particular year. In addition, the publication of book chapters was more noticeable in the year 2017 and 2019.

Productivity

Table 4 illustrates the output of the publications among the continents. It is essential to scrutinise the output growth of the articles in order to analyse the malware issue that is a worldwide concern. These articles were analysed based on the continent category so as to

Table 3 Publication based on the year

Year	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
No. of Publication	1	6	26	60	119	198	241	254	236	137
Publication %	0.1	0.5	2.0	4.7	9.3	15.5	18.8	19.9	18.5	10.7



	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Articles	1	1	3	7	22	51	58	68	101	102
Journal	0	5	23	54	99	148	186	187	130	34
Book chapter	0	0	0	0	0	0	0	2	0	3

Fig. 2 Numbers of publication type based on years

detect the awareness of the malware issue and the frequency of malware attacks in the user country. Data presented in Table 4 list the publications across continents from year 2010 to 2019.

Following the analysis of publications across continents, data are subsequently categorised based on countries and continents according to year. Table 5 further illustrates.

From the above, it can be noted that the most productive continent in publishing articles were Asia and Europe. The former produced 40.5% while the latter produced 26.5%, and North America produced 20.3%. It appears that Asia had outperformed Europe by 14%, thereby making Asia the most prolific in publications focusing on Android malware. Among these, 20.1% of publications were from China. Other countries that followed suit include: the United States, India, Italy, and South Korea. Comparatively, the Middle East, Australia, Africa, and South America contributed less.

Research funding is genuinely needed in scientific research. Here, it is observed that the United States had spent around 500 billion USD for research and development (R&D) while China had spent about 400 billion USD (Enago Academy 2018). However, research in the United States remained stagnant due to economic trouble (Enago Academy 2018) whereas China managed to increase its R&D funding, simultaneously yielding the most in scientific research. This is because it had the support of its government with a lot of funding provided for a collaborative venture in China (International Center 2019). In this regard, China defeated the United States, for the first time in science publishing (Enago Academy 2018; Dockrill 2018). Thus, Asia has become the most prolific in the publication of Android malware articles.

Research area

The subsequent finding focused on research areas which discussed the total publications found on a particular research area. This measure is important for measuring the performance and challenges observed in the different fields of studies. The yield of the related research areas uncovered the movement of the research studies. Here, it was noted that the

Table 4 Productivity based on continents

Continent/country	Number of articles	% of articles
South America	17	1.0
Argentina	1	0.1
Brazil	5	0.3
Chile	2	0.1
Colombia	8	0.6
Ecuador	1	0.1
North America	330	20.3
Canada	48	2.9
Mexico	7	0.4
Nicaragua	4	0.2
Russia	6	0.4
United States	272	16.7
Asia	659	40.5
Bangladesh	5	0.3
China	328	20.1
India	110	6.8
Indonesia	4	0.2
Japan	15	0.9
Malaysia	42	2.6
Alestine	2	0.1
Singapore	33	2.0
South Korea	73	4.5
Sri Lanka	1	0.1
Taiwan	33	2.0
Thailand	3	0.2
Vietnam	10	0.6
Europe	431	26.5
Austria	13	0.8
Belgium	3	0.2
Croatia	2	0.1
Cyprus	3	0.2
Czech Republic	5	0.3
Denmark	7	0.4
England	60	3.7
Finland	10	0.6
France	36	2.2
Germany	44	2.7
Greece	14	0.9
Iceland	1	0.1
Italy	98	6.0
Luxembourg	20	1.2
Malta	1	0.1
Myanmar	1	0.1
Netherlands	5	0.3
North Ireland	13	0.8
Norway	2	0.1

Table 4 (continued)

Continent/country	Number of articles	% of articles
Poland	2	0.1
Portugal	6	0.4
Romania	6	0.4
Scotland	8	0.5
Slovakia	2	0.1
Spain	46	2.8
Sweden	9	0.6
Switzerland	11	0.7
Ukraine	1	0.1
Wales	2	0.1
Australia	37	2.3
Australia	35	2.1
New Zealand	2	0.1
Middle East	142	8.7
Algeria	2	0.1
Egypt	3	0.2
Iran	17	1.0
Israel	7	0.4
Jordan	4	0.2
Lebanon	4	0.2
Morocco	2	0.1
Oman	1	0.1
Pakistan	29	1.8
Qatar	5	0.3
Saudi Arabia	24	1.5
Turkey	38	2.3
U Arab Emirates	6	0.4
Africa	12	0.7
Namibia	1	0.1
Nigeria	3	0.2
South Africa	7	0.4
Tunisia	1	0.1

WoS contained 27 research fields in the publication of Android malware. Table 6 presents this outcome.

From the above, the statistics showed that there were numerous research areas that were related, for instance, Computer Science, Engineering, Telecommunication, Science Technology, and Automation Control systems. The publications noted for all these research areas were dominated by Computer Science and Engineering, with 86.1% and 38%, respectively. The total publications for Computer Science involving Android malware issues emerged from the evolution of device technology. Here, it was observed that the total publications from the Computer Science field were 1100 articles, followed by Engineering with 386 articles.

Second to Computer Science, the Engineering field was then followed by the Telecommunications field. Based on this, it can thus be deduced that Computer Science and

Table 5 Productivity of continent based on year

Continent/country	Year									
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
South America	0	0	0	0	1	5	5	0	3	4
Argentina	0	0	0	0	0	0	0	0	0	1
Brazil	0	0	0	0	0	2	1	0	2	0
Chile	0	0	0	0	0	1	1	0	0	0
Colombia	0	0	0	0	1	2	3	0	1	2
Ecuador	0	0	0	0	0	0	0	0	0	1
North America	0	1	9	21	33	54	71	64	62	15
Canada	0	0	2	0	5	11	7	7	11	5
Mexico	0	0	0	0	0	0	5	1	1	0
Nicaragua	0	0	0	0	0	0	1	2	1	0
Russia	0	0	1	0	0	0	0	4	1	0
United States	0	1	6	21	28	43	58	50	48	10
Asia	0	1	8	19	62	97	120	131	139	82
Bangladesh	0	0	0	0	0	1	1	1	2	0
China	0	1	5	7	25	44	59	69	75	43
India	0	0	0	1	12	18	15	25	25	14
Indonesia	0	0	0	0	0	2	1	0	1	0
Japan	0	0	0	1	1	1	3	4	3	2
Malaysia	0	0	0	3	4	4	6	10	12	3
Palestine	0	0	0	1	0	0	0	0	0	1
Singapore	0	0	0	0	1	5	10	7	6	4
South Korea	0	0	0	5	14	14	13	6	11	10
Sri Lanka	0	0	0	0	0	1	0	0	0	0
Taiwan	0	0	2	1	5	7	10	4	2	2
Thailand	0	0	1	0	0	0	2	0	0	0
Vietnam	0	0	0	0	0	0	0	5	2	3
Europe	0	5	10	21	34	63	89	91	77	41
Austria	0	0	1	3	2	1	2	1	1	2
Belgium	0	0	0	0	1	1	1	0	0	0
Croatia	0	0	0	0	0	1	1	0	0	0
Cyprus	0	0	0	0	0	0	1	0	2	0
Czech Republic	0	0	0	0	0	2	1	0	0	2
Denmark	0	0	0	0	1	0	1	1	4	0
England	0	0	1	1	4	6	10	16	15	7
Finland	0	0	1	0	2	1	2	4	0	0
France	0	0	2	2	5	6	4	8	8	1
Germany	0	2	3	4	3	12	8	6	4	2
Greece	0	1	0	0	2	6	1	1	3	0
Iceland	0	0	0	0	1	0	0	0	0	0
Italy	0	1	0	3	7	10	30	19	19	9
Luxembourg	0	0	1	0	2	3	5	7	0	2
Malta	0	0	0	0	0	0	0	0	1	0
Myanmar	0	0	0	0	0	0	1	0	0	0

Table 5 (continued)

Continent/country	Year									
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Netherlands	0	0	0	1	0	0	1	2	1	0
North Ireland	0	0	0	1	2	2	2	2	1	3
Norway	0	0	0	0	0	1	0	0	0	1
Poland	0	0	0	0	0	0	1	1	0	0
Portugal	0	0	0	0	0	0	1	3	1	1
Romania	0	0	0	0	0	3	0	2	1	0
Scotland	0	0	0	1	0	1	5	1	0	0
Slovakia	0	0	0	0	0	1	0	1	0	0
Spain	0	0	1	4	2	5	4	10	12	8
Sweden	0	0	0	1	0	0	2	4	2	0
Switzerland	0	1	0	0	0	1	5	0	1	3
Ukraine	0	0	0	0	0	0	0	1	0	0
Wales	0	0	0	0	0	0	0	1	1	0
Australia	0	0	0	2	2	5	8	2	8	10
Australia	0	0	0	2	2	4	8	2	7	10
New Zealand	0	0	0	0	0	1	0	0	1	0
Middle East	1	0	1	3	7	13	26	27	36	28
Algeria	0	0	0	0	0	0	1	0	1	0
Egypt	0	0	0	0	0	1	0	0	2	0
Iran	0	0	0	1	1	1	2	7	3	2
Israel	1	0	1	1	2	1	1	0	0	0
Jordan	0	0	0	0	0	0	1	1	0	2
Lebanon	0	0	0	1	1	0	1	0	1	0
Morocco	0	0	0	0	0	0	1	0	1	0
Oman	0	0	0	0	0	1	0	0	0	0
Pakistan	0	0	0	0	0	2	7	2	11	7
Qatar	0	0	0	0	0	0	2	2	0	1
Saudi Arabia	0	0	0	0	2	1	3	6	4	8
Turkey	0	0	0	0	1	4	6	8	12	7
U Arab Emirates	0	0	0	0	0	2	1	1	1	1
Africa	0	0	2	0	2	3	0	1	1	3
Namibia	0	0	0	0	0	0	0	0	0	1
Nigeria	0	0	0	0	1	1	0	0	0	1
South Africa	0	0	2	0	1	2	0	0	1	1
Tunisia	0	0	0	0	0	0	0	1	0	0

Engineering correlated with each other. Both contributed to developing a new technology that could be used by academia and the public. Nonetheless, there were specific terms observed to be related to Computer Science and Engineering, for instance, machine learning, security, artificial intelligence, computer architecture, and data processing. The development of new mobile devices was associated with the expertise of Computer Science and Telecommunications, hence their link with each other.

Table 6 Research area of studies

Research areas	Publications	Publication %
Computer Science	1100	86.1
Engineering	486	38.0
Telecommunications	321	25.0
Science Technology Other Topics	28	2.2
Automation Control Systems	28	2.2
Robotics	14	1.2
Mathematics	10	0.8
Physics	10	0.8
Materials Science	7	0.6
Information Science Library Science	5	0.4
Operations Research Management Science	5	0.4
Chemistry	4	0.3
Education Educational Research	3	0.2
Instruments Instrumentation	3	0.2
Acoustics	2	0.2
Energy Fuels	2	0.2
Mechanics	2	0.2
Optics	2	0.2
Business Economics	2	0.2
Fisheries	1	0.1
Health Care Sciences Services	1	0.1
Imaging Science Photographic Technology	1	0.1
Legal Medicine	1	0.1
Mathematical Computational Biology	1	0.1
Medical Informatics	1	0.1
Psychology	1	0.1
Social Sciences Other Topics	1	0.1

The article with the highest citation was traced to Dissecting Android Malware: Characterisation and Evolution with 655 citations under the Computer Science and Engineering area in the WoS database. This confirmed that there was a close connection between the field of Computer Science and Engineering. Consequently, there was no significant difference within the first and second contributors in the publication of Android malware articles. Both areas were correlated in producing articles on the same topics. The rest of the research areas are listed in Table 6.

Web of Science categories

Table 7 lists the WoS categories, which presents the seven (7) sub-categories of Computer Science. The first among these was Computer Science Theory Methods, followed by Computer Science Information System. The other five sub-categories came under the research area of Engineering comprising Electrical Electronics Engineering, Multidisciplinary Engineering, Mechanical Engineering, Industrial Engineering, and Aerospace Engineering.

Table 7 Web of Science categories

WoS category	Publication	% Publication
Computer Science Theory Methods	554	43.4
Computer Science Information Systems	499	39.0
Engineering Electrical Electronic	465	36.4
Telecommunications	319	25.0
Computer Science Software Engineering	211	16.5
Computer Science Artificial Intelligence	162	12.7
Computer Science Hardware Architecture	108	8.5
Computer Science Interdisciplinary Applications	102	8.0
Automation Control Systems	28	2.1
Multidisciplinary Sciences	19	1.5
Engineering Multidisciplinary	18	1.4
Robotics	14	1.1
Computer Science Cybernetics	9	0.7
Mathematics Applied	9	0.7
Physics Applied	8	0.6
Materials Science Multidisciplinary	7	0.6
Logic	6	0.5
Information Science Library Science	5	0.4
Operations Research Management Science	5	0.4
Engineering Mechanical	4	0.3
Mathematics	4	0.3
Chemistry Multidisciplinary	3	0.2
Instruments Instrumentation	3	0.2
Acoustics	2	0.2
Education Educational Research	2	0.2
Education Scientific Disciplines	2	0.2
Energy Fuels	2	0.2
Engineering Industrial	2	0.2
Green Sustainable Science Technology	2	0.2
Mathematics Interdisciplinary Applications	2	0.2
Mechanics	2	0.2
Optics	2	0.2
Business	1	0.1
Chemistry Analytical	1	0.1
Engineering Aerospace	1	0.1
Ergonomics	1	0.1
Fisheries	1	0.1
Health Care Sciences Services	1	0.1
Imaging Science Photographic Technology	1	0.1
Mathematical Computational Biology	1	0.1
Medical Informatics	1	0.1
Medicine Legal	1	0.1
Nanoscience Nanotechnology	1	0.1
Physics Fluids Plasmas	1	0.1

Table 7 (continued)

WoS category	Publication	% Publication
Physics Mathematical	1	0.1
Physics Multidisciplinary	1	0.1
Psychology Experimental	1	0.1
Psychology Multidisciplinary	1	0.1
Social Sciences Interdisciplinary	1	0.1

As is obvious, Electrical Electronics Engineering comprised the most Android malware related publications, while Aerospace Engineering had the lowest.

Author

The finding in terms of the author is significant in this bibliometric study. It facilitates other researchers in their studies by highlighting the most prolific or most active contributor in terms of publications in the Android malware research. Table 8 presents the top 20 most influential and productive authors. The table classified under Author is organised in terms of the number of publications, institutions, and countries.

Table 8 Authors

Authors	Publication	% Publications	Institution	Country
Francesco Mercaldo	33	2.5	University of Sannio	Italy
Fabio Martinelli	20	1.6	University of Sannio	Italy
Mauro Conti	19	1.5	Uni of Padua	Italy
Carraro Aoron Visaggio	18	1.4	University of Sannio	Italy
Jacques Klein	17	1.4	Univ Luxembourg	Luxembourg
Yang Liu	16	1.3	Xidian Univ	China
Nor Badrul Anuar	15	1.2	Univ of Malaya	Malaysia
Li Li	15	1.2	Monash Uni	Australia
Tegawende F Bissyande	14	1.1	Univ Luxembourg	Luxembourg
Zhenxiang Chen	13	1.0	Univ of Jinan	China
Vijay Laxmi	13	1.0	Malaviya Natl Inst Technol	India
Wei Wang	13	1.0	Univ of Beijing	China
Manoj Singh Gaur	12	0.9	Malaviya Natl Inst Technol	India
Le Traon Yves	12	0.9	Univ Luxembourg	Luxembourg
Li Qi	12	0.9	Uni Beijing	China
Vittoria Nardone	11	0.9	University of Sannio	Italy
Sakir Sezer	11	0.9	University Belfast	Ireland
Vinod P	11	0.9	Uni of Padua	Italy
ShanshanWang	10	0.8	Univ of Jinan	China
QibenYan	10	0.8	Univ of Nebraska-Lincoln	United States
Suleiman Y. Yerima	10	0.8	University Belfast	Ireland

Data above highlights publications generated from all the seven continents. Countries like Europe and Asia were the most notable, producing the most publications in Android malware with countries like Italy, Luxembourg, Malaysia, China, and India holding the best record. The top three authors were from the continent of Europe, specifically, from Italy. The most prominent author was Francesco Mercaldo, who published 33 articles, followed by Fabio Martinelli with 20 articles and Mauro Conti with 19 publications. Both Francesco Mercaldo and Fabio Martinelli were from the University of Sanni, whereas Mauro Conti was from the University of Padua. From Asia, Yang Liu, Nor Badrul Anuar, and Vijay Laxmi served as the most active contributors. From China, Yang Li contributed a total of 16 publications while Nor Badrul from the University of Malaya, Malaysia, contributed a total of 15 articles. The top 20 authors who were involved in various research areas were from 16 different institutions.

High cited articles

This section describes the number of citations, as illustrated in Table 9. A list of 25 most cited articles with information in terms of citation numbers, published journal, year, and research areas was presented. The top three contained the most cited publications which were published between five and seven years ago. This information conformed with the theory that the citation came from articles that have been longer in the database (Razak et al. 2016). The research areas contributing to the publications on Android malware include Engineering, Telecommunications, Science Technology other topics, Automation Control Systems, Robotics, Mathematics, and finally, Computer Science which had become the dominant field for highly cited articles.

As noted in Table 9, the article that was most cited was, "Dissecting Android Malware: Characterisation And Evolution" which received 655 citations (Zhou and Jiang 2012). The author of this article was from China, the continent of Asia, and the article was published by the journal of the IEEE Symposium on Security and Privacy in 2012. The article described the characteristics and evolution of malware by presenting a total of 1260 samples of Android malware from 49 dissimilar families. The characteristics of these malware samples were examined based on their behaviours, including installation, activation, and payloads. The article indicated the best detection of the malware at 79.6% and the worst detection at 20.2% based on the dataset. This outcome thus demanded that a better solution be developed for the next generation of mobile malware detection.

The top second article was "Flowdroid: Precise Context, Flow, Field, Object-Sensitive And Lifecycle-Aware Taint Analysis For Android Apps", with 385 citations published in 2014 by Acm Sigplan Notices (Arzt et al. 2014). This article used static taint analysis to present FLOWDROID for Android applications. The experiment was implemented on 500 benign and 1000 malware from Google play and the VirusShare project, respectively. A closer view of both the two articles suggested that researchers studying malware detection could use this information for further knowledge. These articles were the most highly cited and acknowledged by other new researchers based on findings, methods, and ideas.

Institutions

This section discusses the publications that were linked to the respective institution. The aim of doing this was to categorise the institutions by comparing the publications. It

Table 9 Highly cited articles

References	Number of Citation	Journal	Year	Research Area
Zhou and Jiang (2012)	655	2012 IEEE Symposium on Security and Privacy (SP)	2012	Computer Science
Arzt et al. (2014)	385	ACM SIGPLAN Notices	2014	Computer Science
Asaf Shabtai et al. (2012)	281	Journal of Intelligent Information Systems	2012	Computer Science
Wu et al. (2012)	192	Proceedings of the 2012 Seventh Asia Joint Conference on Information Security (ASIAJCIS 2012)	2012	Computer Science
Aafer et al. (2013)	187	Security and Privacy in Communication Networks, SECURECOMM 2013	2013	Computer Science
Davi et al. (2011)	132	Information Security	2011	Computer Science
Zhang et al. (2014)	117	Ccs'14: Proceedings of the 21st ACM Conference on Computer and Communications Security	2014	Computer Science
Faruki et al. (2014)	111	IEEE Communications Surveys and Tutorials	2015	Computer Science
Gorla et al. (2014)	102	36th International Conference on Software Engineering (ICSE 2014)	2014	Computer Science
Feng et al. (2014)	97	22nd ACM SIGSOFT International Symposium on The Foundations of Software Engineering (FSE 2014)	2014	Computer Science
Wei et al. (2014)	96	CCS'14: Proceedings of the 21st ACM Conference on Computer and Communications Security	2014	Computer Science
Peiravian and Zhu (2013)	91	2013 IEEE 25th International Conference on Tools with Artificial Intelligence (ICTAI)	2013	Computer Science
Wang et al. (2014)	82	IEEE Transactions on Information Forensics and Security	2014	Computer Science
Suarez-Tangil et al. (2014)	81	Expert Systems with Applications	2014	Computer Science
Yerima et al. (2013)	81	2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA)	2013	Computer Science
Sanz et al. (2013)	80	International Joint Conference CISIS'12—ICEUTE'12—SOCO'12 Special Sessions	2013	Computer Science
Shabtai et al. (2014a, b)	70	Computers & Security	2014	Computer Science
Seo et al. (2014a, b)	69	Journal of Network and Computer Applications	2014	Computer Science
Yuan et al. (2014)	68	ACM Sigcomm Computer Communication Review	2014	Computer Science
Tam et al. (2017)	66	ACM Computing Surveys	2017	Computer Science
Narudin et al. (2016)	65	Soft Computing	2016	Computer Science
Rastogi et al. (2014)	65	IEEE Transactions on Information Forensics and Security	2014	Computer Science
Zheng et al. (2013)	64	2013 12th IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (TRUSTCOM 2013)	2013	Computer Science
Feizollah et al. (2015)	63	Digital Investigation	2015	Computer Science

Table 9 (continued)

References	Number of Citation	Journal	Year	Research Area
Yuan et al. (2016)	61	Tsinghua Science and Technology	2016	Computer Science

Table 10 Institutions

Institutions	Publications	% Publication	Country
Chinese Academy of Sciences	47	3.7	China
Beijing University of Posts Telecommunications	33	2.6	China
Consiglio Nazionale Delle Ricerche Cnr	28	2.2	Italy
University of Sannio	26	2.0	Italy
Institute of Information Engineering Cas	25	2.0	China
Istituto Di Informatica E Telematica Iit Cnr	23	1.8	China
University of Chinese Academy of Sciences Cas	21	1.6	China
Tsinghua University	20	1.6	China
University of London	20	1.6	England
University of Luxembourg	20	1.6	Luxembourg
University of Padua	19	1.5	Italy
Pennsylvania Commonwealth System of Higher Education	19	1.5	United States
Universiti Malaya	17	1.3	Malaysia
University of California System	16	1.3	United States
University System of Georgia	16	1.3	United States
Korea University	15	1.2	Korea
University of Jinan	15	1.2	China
Nanyang Technological University	14	1.1	Singapore
Nanyang Technological University National Institute of Education Nie Singapore	14	1.1	Singapore
Centre National De La Recherche Scientifique	13	1.0	France
State University System of Florida	13	1.0	United States
Gazi University	12	0.9	Turkey
Inria	12	0.9	France
Malaviya National Institute of Technology Jaipur	12	0.9	India
Queens University Belfast	12	0.9	North island
Royal Holloway University London	12	0.9	England
University of New Brunswick	12	0.9	Canada
University of North Carolina	12	0.9	United State
University of Texas System	12	0.9	United State

was found that institutions from Asia held the highest in Android malware publications. Table 10 illustrates the top 30 of the greatest institution, comprising four continents: Asia, Europe, the Middle East, and North America.

Table 10 presents the most distinguished institutions in publishing Android malware articles. It is noted that the Chinese Academy of Science is the greatest institution for publication, followed by Beijing University. This also showed that institutions from the continent of Asia had the greatest number of publications. This was then followed by other institutions from the continent of Europe, followed in line by North America.

Other distinguished institutions that were from Asia include the University of Chinese Academy, Tsinghua University, University of Malaya, Korea University, and the University of Jinan. This study further discovered that most eminent institutions in Asia were located in China. Moreover, China's speed in the publication surpassed other countries in Asia, with mainly seven (7) institutions that contributed to these publications. Moreover,

the analysis showed that the entire publications among institutions were held together by a small gap. Slightly different publications among the institutions proved that the researchers had excellent facility and high competition.

Impact journal

This section discusses the impact of the journal under the Computer Science field. A journal is a publication comprising of articles written by researchers and experts in a specific field of study and solely for academic or technical purposes. The impact journal is one of the critical parts in this study as it represents the most prominent journal with the greatest citations received in publications. The most influential journals are shown in Table 11 with the quartile, numbers of citation, impact factor, and average citations per year.

From the top 20 highest impact journal articles of Android malware, there were eight (8) articles with Quartile 1 (Q1) impact. Q1 to Q4 refers to journal's ranking quartiles within a subdiscipline. Q1 is the greatest impact of the journal. In this regard, the most influential journal in this study was the IEEE Communications Surveys and Tutorials that have been in the WoS for five (5) years. It has an average of 22.2 citations per year. The title of the best impact journal article in the WoS was: Android Security: A Survey of Issues, Malware Penetration, and Defenses with 111 citations. Moreover, the oldest journal in the WoS is the Journal of Systems and Software which has been in the WoS for ten years. It has 44 citations and an average of 4.4 citations per year. Aforementioned, the number of journals for Quartile 2 (Q2) is two (2), and for Quartile 3 is seven (7).

Figure 3 illustrates the top 20 authors, with 17 countries, and 28 of the most used keywords. As seen in the figure, China is the highest contributor to the publication of an article with 12 authors. Next in line is Italy, the United States, India, and Luxembourg. There seemed to be a significant difference between the first contributor, China, and the second contributor, Italy. The most common keywords used by the authors were: malware, Android, malware detection, and machine learning. Likewise, Malaysia also contributed to the publication, with the keyword most used being Android. The figure shows that the continent of Asia is the most prolific contributor to the production of Android malware, with studies conducted in China, Malaysia, India, and Singapore.

Figure 4 illustrates the relationship between the title, the authors and their affiliations. The titles most frequently used by the authors are Android, malware, and detection, and this applies to all the institutions. The title less used by the authors were framework, dynamic classification, approach, and techniques. Yang Liu from China was the top author, as seen in the figure. He also used the keyword Android in the title of his articles. The top university noted in Fig. 4 is traced to the University of Chinese Academy Science from China. Likewise, the University of Malaya, and the University of Malaysia Pahang, from Malaysia, also contributed to this publication on Android malware.

Malware intrusion detection system (IDS)

This section describes the malware IDS used as a methodology in malware detection. Malware is purposely created to disrupt the computer or mobile devices so as to gain information and to spread the virus to infect the devices. Android has a size of 3.5 million applications and 99% have been targeted by malware (Amin et al. 2020). Most of the antivirus

Table 11 Impact journal of Android malware articles

Journal	Q	C	IF	Year	ACP	References
IEEE Communications Surveys and Tutorials	Q1	111	22.973	2015	22.2	Faruki et al. (2014)
IEEE Transactions on Information Forensics and Security	Q1	82	6.211	2014	13.67	Wang et al. (2014)
Expert Systems with Applications	Q1	81	4.292	2014	13.5	Suarez-Tangil et al. (2014)
Journal of Network and Computer Applications	Q1	69	5.273	2014	11.5	Seo et al. (2014a, b)
ACM Computing Surveys	Q1	66	6.131	2017	222	Tam et al. (2017)
IEEE Transactions on Information Forensics and Security	Q1	65	6.211	2014	10.83	Rastogi et al. (2014)
IEEE Transactions on Industrial Informatics	Q1	46	7.377	2018	23	Li et al. (2018)
Journal of Systems and Software	Q1	44	2.559	2010	4.4	Asaf Shabtai et al. (2010)
Soft Computing	Q2	65	2.784	2016	16.25	Narudin et al. (2016)
Computers & Security	Q2	70	3.062	2014	11.67	Shabtai et al. (2014a, b)
Journal of Intelligent Information Systems	Q3	281	1.589	2012	35.13	Asaf Shabtai et al. (2012)
ACM Sigcomm Computer Communication Review	Q3	68	1.74	2014	11.33	Yuan et al. (2014)
Digital Investigation	Q3	63	1.66	2015	12.6	Feizollah et al. (2015)
Tsinghua Science and Technology	Q3	63	1.696	2016	15.75	Yuan et al. (2016)
Digital Investigation	Q3	56	1.66	2015	11.2	Talha et al. (2015)
IET Information Security	Q3	52	0.949	2014	8.7	Yerima et al. (2014)
IET Information Security	Q3	47	0.949	2015	9.4	Yerima et al. (2015)
ACM SIGPLAN Notices	Q4	385	0.335	2014	64.17	Arzt et al. (2014)
Information Security	Q4	132	0.402	2011	14.67	Davi et al. (2011)
Computer Security—Esorics	Q4	57	0.402	2014	9.5	Yang et al. (2014)

Q quartile, *C* citation, *IF* impact factor, *ACP* average citation per year

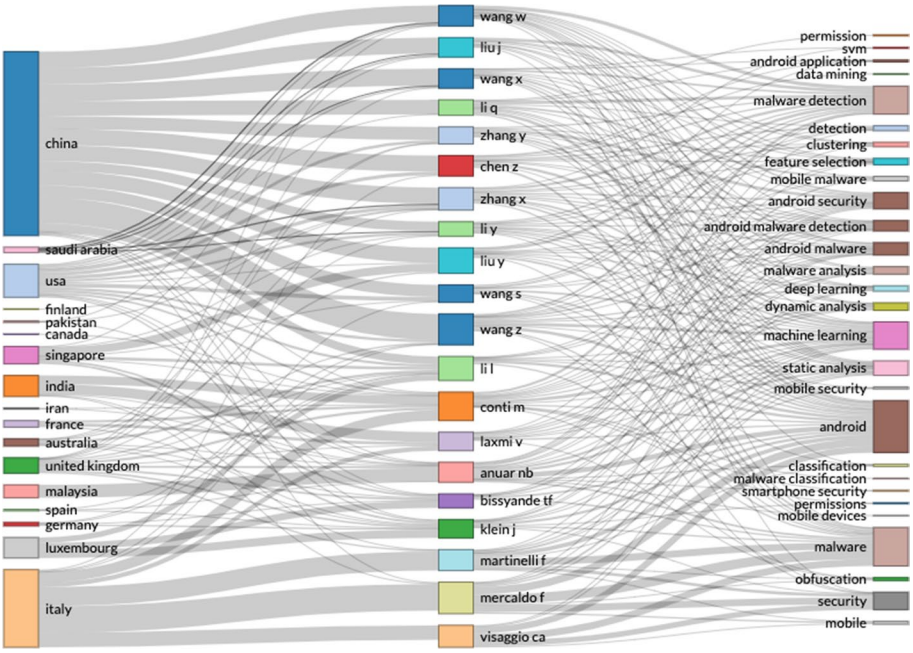


Fig. 3 Relationship between country, author, and keywords

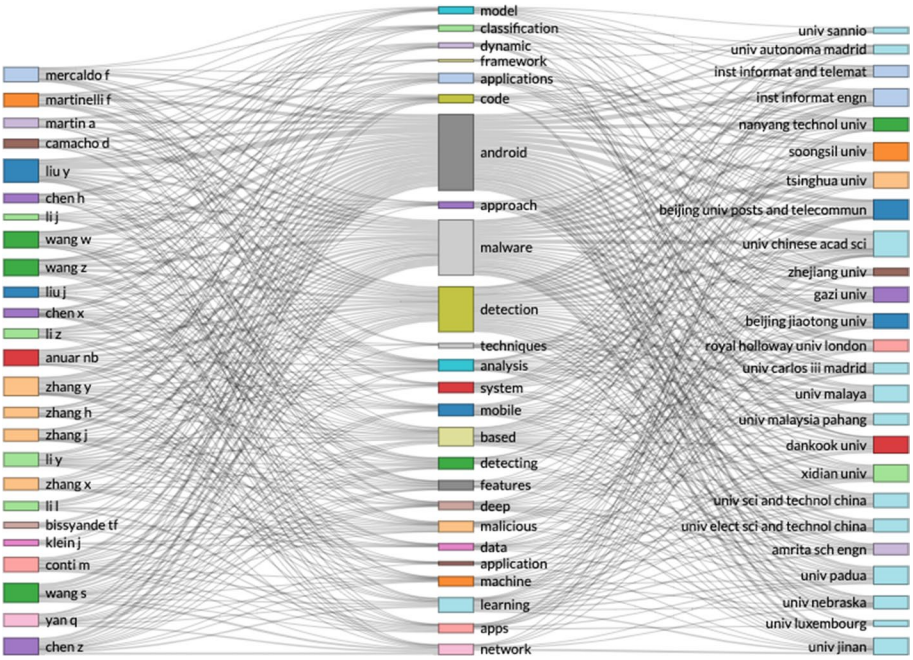


Fig. 4 Relationship between title with author and affiliation

provided in Android apps do nothing to check the malware behaviour (Whitwam 2020). On top of that, 21.1 million Android mobile devices have been affected by malware applications when mobile users downloaded applications from Google Play Store (Counterpoint 2019). This malware will indirectly influence users to adhere to unwanted premium services, thereby causing severe damages to the mobile device (Computer Hope 2019). Malware applications calmly kidnap users' account details, making users subscribe to premium messages via SMS, and then compromising the hardware (The App Store Celebrates 10 Years and 2 Million Apps 2018). Mobile devices usually contain a lot of personal data and crucial information that are often used for online transactions, and as a medium for bill payments (Wazid et al. 2019), thereby leading to many financial transactions. The impact of the malware is that it would conduct all these activities silently without the mobile device users' knowledge, causing users' financial losses. Some methods have been introduced to help researchers detect and overcome malware presence. Amin et al. (2020) proposed Android Intent (implicit and explicit) for malware detection by combining the Android permission and Android Intent. The use of intent continued in study (Shrivastava and Kumar 2019a) which focused on permission and intent modelling. On the other hand, Taheri et al. (2020) developed four detection methods using Hamming distance to find the similarities of benign and malware samples. Those mentioned studies used static analysis technique which is considered the greatest method in reducing power and time consumption in detecting the malware. Despite that, Garg et al. (2020) proposed a multi stage model using anomaly (dynamic) to solve the security of IoT-enabled application. Both techniques have different roles and advantages.

Malware detection system is divided into three (3) sections as illustrated in Fig. 5. This system includes the analysis techniques, the detection approaches, and the deployment approaches.

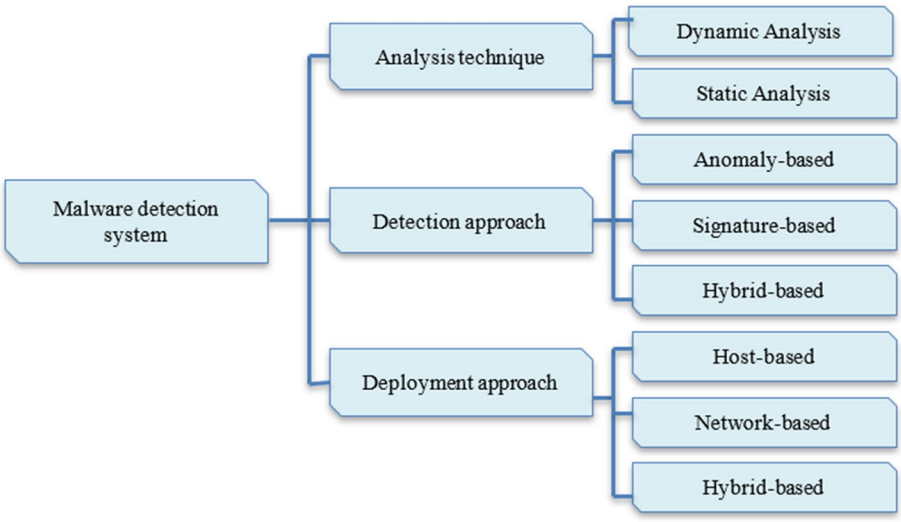


Fig. 5 Taxonomy of the malware detection system

Analysis technique

Analysis technique is a method which can determine the malicious code by classifying the malware features into two types: dynamic analysis and static analysis (Belaoued et al. 2019). Both types of analysis techniques are used to detect malware presence. Unfortunately, the unscrupulous author can use obfuscation as a technique to prevent being detected (Or-Meir et al. 2019). Obfuscation is a technique practiced so as to make something difficult to understand.

Static analysis is a technique of investigating the code in offline mode (Amin et al. 2020). The examination is executed without running an application (Amin et al. 2020; Statista 2019; Tam et al. 2017; Akour et al. 2017). For this purpose, it uses the reverse engineering technique to extract certain features for analysis, such as API and data permissions (Singhal et al. 2019). Static analysis detects the malware by comparing the detection code with the source code in the database. The process of the static analysis reads the code and detects unfamiliar code as malware. Studies by Singhal et al. (2019) and Magdum (2015) have detected malware by using static analysis technique. The advantage of using static analysis is its fast detection. The process of detection can be performed without executing the applications (Shrivastava and Kumar 2017). Although static analysis is unable to detect the obfuscation technique, it is able to reveal and address the suspicious files much faster (Shrivastava and Kumar 2019a).

Dynamic analysis observes the behaviour of malicious files during the execution of an application (Akour et al. 2017). It is different from static analysis in that dynamic analysis is able to detect unknown malware, new malware, and even obfuscation techniques (Kuntz et al. 2017; Kim et al. 2019). The application that is detected as malicious by static analysis will then be re-analysed by dynamic analysis. This technique is more accurate and it reduces costs. Some studies such as Lanet et al. (2018) and Feizollah et al. (2017) had used dynamic analysis. The only limitation of dynamic analysis is that

Table 12 The comparison between static and dynamic analyses

Analysis technique	Static	Dynamic
Characteristic		
Analysis mode	Offline mode	In execution of applications
Malware analysis	Applied Reverse engineering tools such as Apktool Using the API system to check malicious	Analyze the behavior during execution of an application It observes the malicious and error program
Tools used for analysis	DroidRanger Scandroid RiskRanker Stowaway AdRisk DNADroid Kirin	CrowDroid TaintDroid ParanoidAndroid Aurasium AppFence DriodScope
Benefit	The detection is fast	The result is more accurate
Limitation	It is incapable of detecting unfamiliar and new malware families	Increase power consumption and cost

it is unable to identify malicious applications like IMEI stealers (Singhal et al. 2019). Table 12 illustrates the comparison between static and dynamic analyses.

Detection approach

Malware detection approaches can be divided into three types: signature, anomaly, and hybrid (Razak et al. 2016). The signature approach detects malware events by matching the signature stored in the database via the normal and abnormal patterns (Seo et al. 2014a, b). In comparison, the anomaly approach recognises malicious behaviours by supervising the events via network traffic and system (Suárez-Tangil et al. 2018). It has the advantage of detecting new malware and unfamiliar malware by observing the behaviour. Nevertheless, this approach is unable to detect unfamiliar and new malware that is not matched with the signature in the database. Thus, the database needs to be updated frequently in order to enable the detection of various malware. The comparison between the signature and anomaly approaches is presented in Table 13.

Another approach is the hybrid approach which is the combination of the anomaly and signature approaches. The combination helps to enable the detection of new malware whenever the signature is unable to perform the detection. This approach overcomes the deficiency of both the anomaly and signature approaches. The studies by Seo et al. (2014a, b) and Yu et al. (2013) had used the anomaly approach to detect malware. Table 14 demonstrates the studies of the signature approach, Table 15 highlights studies of the anomaly approach and Table 16 presents the studies of the hybrid approach.

Deployment approach

The deployment approach is used for detecting malware in the intrusion detection system (IDS). An IDS is a security tool used for recognising intrusions, just like the firewall (Feizollah et al. 2013). The IDS hardware, software, or combination, is used for monitoring the activities and for detecting the malware signal in the network or system. Anomaly detection and signature-based detection are two types of IDSs (Daimi 2017). The malware intrusion

Table 13 The comparison between signature and anomaly approaches

Detection approach	Advantages	Disadvantages
Signature	High detection rate and accuracy for known attacks The simple and effective to detect known malware Has lower false alarm rate	Only detect the code that has a signature in the database The database needs to update frequently to detect new malware
Anomaly	Able to adapt and detect new, unique and abnormal malware Less dependent on an existing database	Have a higher false alarm rate due to unconfigured properly before their deployment

Table 14 Signature approach

References	Aim	Classifier	Performance
Almin and Chatterjee (2015)	To propose an Android application analyzer (AAA) to identify malicious applications installed on the phone	K-Means and Naïve Bayesian	More Accurate Compared To The Anti-Virus
Sheen et al. (2015)	To design scalable mechanisms using multi-feature collaborative decision fusion (MCDF)	Naïve Bayes, J48, SVM and Ibk	TPR = 97%, Precision = 83%
Sharma and Gupta (2019)	To propose a method using machine learning for privacy risk analysis in Android applications	Bayesian network	Accuracy = 95.5%
Zhu et al. (2018)	To propose DroidDet with low cost and high efficient	Rotation forest and SVM	Accuracy = 88.3%
Martín et al. (2019)	To analyze malware using Machine learning classifier	Graph-Community Algorithm and Hierarchical Clustering	Accuracy = 84%

SVM support vendor machine

Table 15 Anomaly approach

References	Objective	Algorithm	Result
An et al. (2018)	To create a robust malware detection to secure home routers	SVM	TPR = 99.8%
Yu et al. (2013)	To analyze Android application behavior using the Machine Learning method. (Dynamic)	Naïve Bayesian with Chi-square	Accuracy = 80.4%
Lanet et al. (2018)	To compare the performance of different detection approaches using different featured	SVM, HMM, (J48), and RF	HMM = 90.64% SVM = 97.33% J48 = 97% RF = 97.33%
Tahir et al. (2019)	To define and propose a new method for recognizing abnormal behaviors in network	LOC and SVM	TPR = 94.8%
Hu et al. (2018)	To propose a combination of network traffic analysis and data mining to classify malicious network behavior	SVM, KNN, and LOF	Accuracy = 81.8%

SVM support vendor machine, *HMM* hidden Markov model, *RF* random forest, *LOF* local outlier factor, *KNN* K-nearest neighbors

Table 16 Hybrid approach

References	Objective	Algorithm	Result
Rehman et al. (2018)	To present detection of malware in Android Applications using signature and anomaly approach	KNN, J48, SVM, decision tree	Accuracy = 99.8%
Ali (2019)	To present a genetic algorithm (GA) and a particle swarm optimization (PSO) to fix up the optimization problem in SVM	GA and PSO	TPR = 96%
Venkatraman et al. (2019)	To examine the proposed method of hybrid image-based with deep learning architectures for effective malware classification	SVM	Accuracy = 98.6%
Adebayo and Aziz (2019)	To improve the malicious detection rate using PSO algorithm against Android	PSO	PSO Accuracy = 98.2%
Huda et al. (2018)	To introduce a hybrid structure to classify features of a large-time routine of malware behavior	SVM	Accuracy = 97.7%

SVM support vendor machine, *LOF* local outlier factor, *KNN* K-nearest neighbors, *GA* genetic algorithm, *PSO* particle swarm optimization

Table 17 Deployment and detection approach studies

References	Deployment Approach	Detection Approach	Year
Guanghui (2020)	NIDS	Anomaly	2020
Yang et al. (2019)	NIDS	Anomaly	2019
Niazi and Faheem (2019)	NIDS	Anomaly	2019
Liang et al. (2019)	NIDS	Anomaly	2019
Besharati et al. (2018)	HIDS	Signature	2019
Jose et al. (2018)	HIDS	Anomaly	2018
Deshpande et al. (2018)	HIDS	Anomaly	2018
Subba et al. (2017)	HIDS	Anomaly	2017
(Haider et al. (2016)	HIDS	Anomaly	2016
Moon et al. (2016)	HIDS	Anomaly	2016
Koucham et al. (2015)	HIDS	Anomaly	2015

Table 18 Malware and the characteristics

Types of malware	Characteristic
Virus	The virus spreads and infects the file and the program by executed itself
Worm	A worm replicates and sending itself through the network without affecting the operating system
Trojan horse	Trojan will disguise itself as a trustworthy program to attract a user to run it. It will distribute the virus when the program is running
Botnet	A Botnet spread itself through the network and allowed an attacker to control the infected computer
Spyware	Spyware took user information, data, and observe their activities without their knowledge
Rootkits	A rootkit treats the root of the system
Adware	Adware is an unwanted advertisement in the form of a popup or banner, and it comes from the history of the user's browser

detection system is deployed either in a host-based, network-based, or hybrid-based system. An activity in the host-based system (HIDS) is monitored, analysed, and processed by itself whilst the deployment detection in network-based (NIDS) system is run by a remote server (Mas'ud et al. 2014a, b). Meanwhile, the hybrid-based detection system comes from the combination of the HIDS and the NIDS. The aim of the combination (HIDS and NIDS) is to increase the capabilities of the existing IDS (Potteti and Parati 2015). The deployment approach used by previous studies is presented in Table 17.

Mobile malware

The popularity of the mobile device has spurred the emergence of malware. Most malware target Androids for spreading the malicious code because it is the most commonly used operating system in many mobile devices. As mentioned before, malware targets mobile activities by stealing user-sensitive data such by encrypting users' banking data, eliminating crucial data, altering, and monitoring user's activities without the users' knowledge (Qamar et al. 2019; Arabo and Pranggono 2013). Malware is able to interrupt

the operation of the devices by consuming the resources of the devices such as the storage, processor, and network (Shrivastava and Kumar 2019b) (*Cyber Secur. Parallel Distrib. Comput.* 2019). The malware author has a lot of creativity such that they spread the malware by infecting the devices and network insidiously. To better understand malware threats, this section reviews studies of mobile malware extracted from the WoS database, published from 2010 to 2019. Table 18 lists the various types of malware and its characteristics which are incredibly harmful to mobile devices. These diverse types of malware can threaten the devices by employing different purposes in order to damage the system in the mobile devices.

The table indicates how each malware type can attack the mobile devices through varying methods. The infected and damaged mobile devices would then be infiltrated with fake emails, unnecessary software updates, fake websites, and counterfeit applications. Their presence is unnoticed because they are silent; thus, devices would be infected without the user's knowledge. Users would only detect their presence when the devices are fully damaged, or in critical condition. Future studies should attempt to describe the detection using multiple methods so as to reduce such incidences on mobile devices. Figure 6 presents the mapping of malicious malware types and their behaviours.

Risk analysis

Risk analysis is a process used to identify the loss, the threat, and the level of risk occurring (Alali et al. 2018). The level of risk is measured based on the impact of the mobile attack. As mobile device functions grow drastically to compete with the new emergence of design among developers in the market place, mobile users face higher risks (Naga

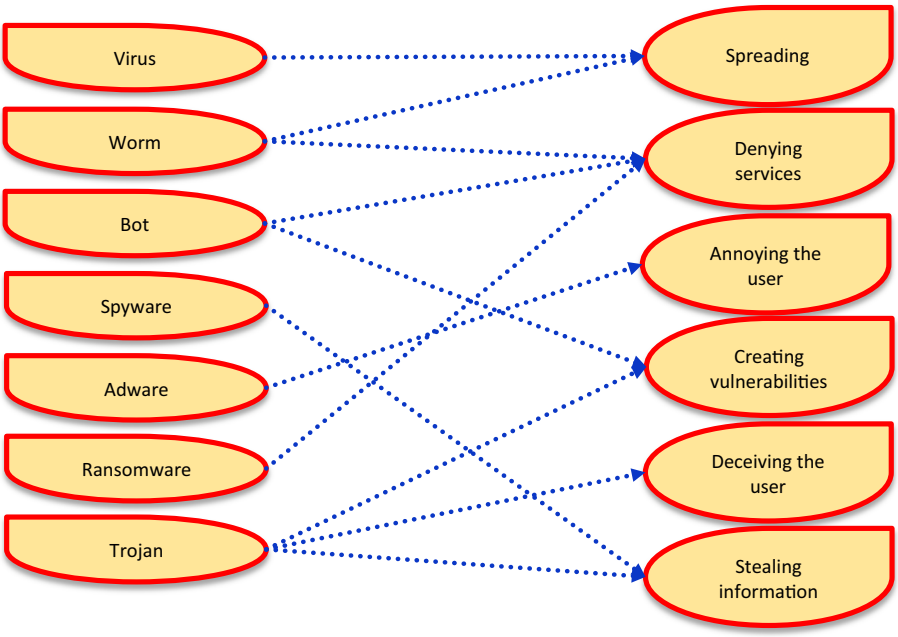


Fig. 6 The mapping of malicious malware types and their behaviours

Table 19 Risk level

Risk level	Description
High	The risk is unacceptable and it reduces the risk implemented before running the application. The data are exposed to leakage, unsecured wifi, the presence of spyware, and phishing attacks
Medium	The risk is acceptable and under protection. It needs to monitor continuously for each threat to ensure the level at the normal
Low	The risk is acceptable and able to be used. The security is provided by the mobile devices with the relevant protection but needs to observe the threat to detect any changes that will increase the risk level

Table 20 The threat and descriptions

Threat	Description
Application based	The threat comes from downloaded applications from the market store. The fraudulent application looks legitimate and exploits the devices once downloaded. The vulnerabilities of the devices contribute to the exploitation of the threat
Web based	The connection of the Internet has spurred the threat easily comes when the users used the devices to surf the website contained malware
Network based	The attackers usually provided open wifi to gain confidential information from the users
Physical based	The portable device easily lost or stolen. The value of the devices gathered with the data stored inside has encouraged the unscrupulous to get the devices physically

Malleswari et al. 2017). Risk analysis is thus analysed by some procedures, such as categorising the risk, triggers, effects of the risk, re-evaluating the possibility of the risk, and finding the factor to mitigate the risk (Sharma and Gupta 2018b; B 2018). There are three levels of risk, such as low, medium, and high (Shrivastava and Kumar 2019c). Likewise, there are three main elements of security materials, such as confidential data, availability, and integrity (B 2018). Table 19 illustrates the risk level of risk analysis.

The risk levels are the yield of the inacceptable effect of ambiguous events or impact of the event. The risk levels are evaluated based on the factor of impact and likelihood. Nevertheless, the vulnerabilities of this method are that they are unable to incorporate the abilities of the threat so as to determine the risk level. Moreover, the threat depends on the vulnerabilities of the system. Therefore, risk analysis helps the user to manage the risk factor for a specific event.

Threats

The risk analysis is the consequence of the threat on mobile devices. Mobile threats are divided into four (4) classes, such as application threats, web threats, network threats, and physical threats (Lookout 2019). Table 20 represents the details of each threat.

Evaluation measure

The common evaluation of measurements as practiced by researchers in malware IDS is the effectiveness of the system they used. This evaluation focuses on accuracy, true positive rate (TPR), false positive rate (FPR), true negative rate (TNR), false negative rate (FNR), f-measure, and recall. A true positive (TP) indicates the precise measurement of the presence of malware. The higher the true positive, the better the outcome. A false negative (FN) indicates a detection of malware erroneously defined as benign. A true negative (TN) refers the benign correctly as a benign while a false positive (FP) defines a benign erroneously as a malware (Kamesh and Sakthi Priya 2012).

Challenges and future direction

The challenges and movements for future research that are related to mobile malware are hereby also discussed. A number of studies had emphasised the malware issue which posed a threat to mobile devices. It is thus a challenge to many researchers looking at malware detection. Although numerous methods have been noted in advanced studies, and various systems have been proposed for detecting malware automatically, malicious files, websites and the number of malware continue to grow (Akour et al. 2017). Thus, more needs to be done in this research field.

Accuracy

The accuracy of malware detection is measured by using the measurement of TP, FP, TN, and FN. They are called true if the detection is accurate and matches reality. The perfect detection is when the TPR = 100%, TNR = 100, FPR = 0% and FNR = 0%. In truth, it is impossible to achieve 100% accuracy of TP and FN (Akour et al. 2017). However, with a larger amount of data, analysis may possibly provide a near accuracy of the positive or negative measurement. False positive or false negative is likewise known as a false alarm. It incorrectly identifies a legitimate programme as a malicious programme or a malicious programme as a legitimate program. This is a big challenge in the IDS. This issue frustrates users and the developers when the programme they had created is blocked. This occurrence can affect the reputation of their business. No one will run the programme anymore when it is flagged as malicious. Another effect for a false alarm is that it could turn the device to become dangerous when the suspicious programme runs into the user device. This scenario is a significant problem in current technology. A study by Wang et al. (2018) uses a hybrid approach to analyse the data of malware, and the results showed a lower rate of false alarm.

Features

Features are the first part to be selected prior to analysing and detecting the malware. The best feature selected would allow the detector to become more efficient (Aung and Zaw 2013). Inappropriate features may cause a high false alarm (Razak et al. 2016). However, the number of features can be reduced so as to get a higher level of accuracy. The first and crucial step in machine learning method is feature selection (Feizollah et al. 2015). The selection of appropriate features can thus lead to higher accuracy, thereby reducing

the false alarm. Nevertheless, accumulating a massive number of inappropriate features for the machine learning classification may cause classifier drawbacks like the misunderstanding of algorithm learning, an increase in the model's running time, and lower generality (Mas'ud et al. 2014a, b). Subsequently, an enormous size of features contributes to the growth of space usage, and intricacy management. Therefore, it is unsuitable for mobile devices with limited storage and restricted power consumption. The selection of appropriate features enables machine learning classifiers to make more efficient detections during the pre-processing of data. Thus, reducing the features is necessary in order to preserve the accuracy.

Dataset

The occurrence of Android malware attacking users has increased rapidly in recent years. The Android malware applies sophisticated techniques such as metamorphism, polymorphism, oligomorphic, obfuscation, and modification to avoid detection. The detection mechanism provided by mobile devices is unable to operate efficiently due to restricted datasets, and the lack of understanding of malicious activities. To evaluate the proposed system of detection, a dataset base is required. The limitation of the malware sample can make the detection system unreliable. This study Razak et al. (2016) discovered that more than 100,000 malware modifications belonged to 777 families. Studies by Zhou and Jiang (2012) and Arzt et al. (2014) had used malware samples from the Virus Share project, and benign samples from Google Play. They noted that the dataset of malware has been proliferating. Based on this, a restriction mechanism is needed. Moreover, outdated dataset has also become inappropriate for analysis, thus research also requires the latest dataset to be examined so as to improve the detection performance in terms of accuracy and to lower the rate of false alarms.

Risk assessment

Risk assessment is a fundamental method used for explaining the possibility of risk levels. It is a crucial part that shields the user against dangerous applications; it grants mobile users a possibility of reducing the threat impact to a tolerable level. The process for risk assessment is carried out so as to measure the impact of the threat based on the value of the assets, threats, vulnerabilities, and the effects resulting from the attack. The acknowledged risk from threats and weaknesses must be ranked depending on the criticality of the issue.

Leading a risk assessment is interesting due to less awareness on its effect on risk decision making. A study by Naga Malleswari et al. (2017) helped to improve users' awareness by presenting the privacy risk for users before granting permission. Similarly, a study by Alali et al. (2018) proposed the Fuzzy Inference Model (FIS) which determines four (4) factors of risk: threat, vulnerability, impact, and likelihood. These were used for classifying the risk impact, and for providing the response to mitigate the risk. Razak et al. (2019) also presented the risk factor based on zoning approaches.

Android malware on the Internet of Things (IoT)

The IoT is the modernised technology of communication among things and objects (Wu et al. 2019). The IoT integrates widely with mobile devices by serving various services

around the world. The mobile devices supervise and control the provided services for the long distance with keyless mechanisms. For example, Macmanus (2012) offered a location in Audi's new business car. The volume of data produced every day from different IoT has enlarged, from terabytes to petabytes (Garg et al. 2020). The IoT services produce more convenient experiences such as remote monitors to lessen energy waste for home equipment, such as air conditioning, television, and refrigerator. With the sharp growth of technology, more and more IoTs services are controlled by Android mobile applications.

Behind the sophisticated technology of IoT, the issue of security in IoT services has also worsened, especially with malware attacks. Likewise, the IoT threat has also increased over the past few years. Attackers are able to slip into mobile user devices and reach the control of the IoT. It benefits the attacker by acquiring and integrating information such as personal data, contact number, location, payment data of Internet banking from mobile devices. The open-source in the Android application has become one of the factors causing malware increase in the IoT services. Studies showed that eight new malware families that emerged in the year 2015 had mostly originated from China and the United States (Johnson 2016).

To overcome the malware attack, some protection has been introduced. However, the protection of the IoT system is actually a part of the tough problem due to the difficulty in developing an effective detection system and in avoiding the leakage of information. The study by Park et al. (2019) proposed three levels of awareness to be introduced into the IoT system: define the threat, measure the risk, and optimise the risk. A study by Wu et al. (2019) was able to detect malware by using the Bayesian network which was grounded on traffic feature analysis. The result showed a higher accuracy with fewer substantial features. Another study (Ham et al. 2014) used the linear support vector machine (SVM) to detect malware so as to secure a reliable IoT service. Another study (Garg et al. 2020) used the Density-Based Spatial Clustering of Applications with Noise for the same purpose.

Mobile banking

The successful use of mobile phone among people and network thriving globally has encouraged the people to expose their business to online systems (Sharma and Gupta 2016). Exposing the business has to expand the users of mobile banking. Despite the advantages of using mobile banking, this type of banking also invites the proliferation of malware altogether. The emergence of banking malware necessitates more attention as this threat is one of the most dangerous threats to the mobile user; e.g. by generating malicious code with the intention of stealing personal financial information from banking and transferring funds activities to the hacker accounts. Mobile bankers previously spread the malware through third-party apps and recently infiltrate Google Play widely (Mobliciti 2020). A new version of mobile banking malware is impersonating as legitimate cryptocurrency wallet to steal money from the secure wallet found on Google Play (Seals 2020; Whittaker 2019). The malware will flourish more in sophistication as cryptocurrency trading becomes widespread.

Fake applications for COVID-19 pandemic

Covid-19 has threatened the world since 2019 and in this period, malware have been growing fast. Ransomware thrives 72% and mobile vulnerabilities grow 50% (Security 2020). This increase in malware is because most of world population is in lockdown, whereby this situation renders developers the busiest in gaining profit for their benefit.

This complicated situation has offered attackers to highlight their talent of creating applications for users. Starting with fake application to control the dissemination of the coronavirus, malicious apps were also created to give recommendations on how to avoid infection from the biological virus. Users would show unlimited interest in any application that are related to COVID-19 in order to stay healthy (Moran 2020). Banking is a susceptible sector in this pandemic since users tend to utilise online shopping during lockdown situations. Banking trojan and information stealers were found rampant with the increase of unemployment (Ljubas 2020). Thus, this sector has contributed to the greatest amount of malware activities to spread malice during the COVID-19 pandemic.

Conclusion

The popularity of computers and mobile devices has led to the emergence of new malware. According to TMS (2011), malware had increased by 54% in 2017 as compared to previous years. A total of 24,000 malicious files are detected each day. An estimation by (Spring 2019) noted that one out of five computers would be attacked by at least one malware in 2019. The Internet is one of the factors frequently spreading malware into user's devices. To alleviate malware problems and to improve safety in mobile devices, several approaches have been introduced by various studies.

The current study used the bibliometric technique to analyse the Android malware trends from 2010 until 2019. Some findings were noted and highlighted, for instance, productivity, research area, authors, highly cited articles, institutions, and impact journals. These criteria were able to highlight the research trends related to Android malware production. The number of Android malware production had increased at an average rate of 2.1% on a yearly basis. The report by Dobran (2019) stated that ransomware attacked new organisations every 14 s for the year 2019, and for the year 2021, it would be every 11 s.

The bibliometric analysis of the Android malware in 2010 until 2019 showed that Asia was the highest contributor of research publications, among other continents. Next was Europe and North America. The Middle East, Australia, Africa, and South America contributed less. The highest publication of Android malware articles was from China, with a total of 25% publications, followed by the United States, India, Italy, and South Korea. This implies that Asia had outperformed Europe by a difference of 17.6% of publications.

In addition, this study has also highlighted the top 20 authors who were most active in the area of research. The top author was Francesco Mercaldo, followed by Fabio Martinelli, Mauro Conti, and Carraro Aaron Visaggio. These top four authors were from Italy, the continent of Europe. The top two authors and the fourth top author were from the University of Sannio while the third top author was from the University of Padua. The subsequent authors were from the countries of Luxembourg, Malaysia, China, and India.

This study has shown the bibliometric analysis of the publications in the field of Android malware. The analysis provides the objective and a quantitative measure of the influence that a publication has on its respective specialty. The information present in this study is important for researchers to build the network of research in their field of study. It is hoped that the information would encourage more future research to be performed as a

measure to overcome the rapid proliferation of malware. Finally, this study delivers a general depiction on the subject matter and aims to exhibit the importance of the expansion in the field of Android malware investigation.

Acknowledgements The work is funded by the Ministry of Higher Education FRGS under Project ID: RACER/1/2019/ICT03/UMP//2 (RDU192613) and UIC190807. The authors thank anonymous reviewers for their constructive comments, and University Malaysia Pahang for the support.

References

Aafer, Y., Du, W., & Yin, H. (2013). DroidAPIMiner: Mining API-level features for robust malware detection in android. In M. Zia, T. Zomaya, A. Varadharajan, & V. Mao (Eds.), *Security and privacy in communication networks, Securecomm 2013* (Vol. 127, pp. 86–103). New York: Springer.

Adebayo, O. S., & Aziz, N. A. (2019). Improved malware detection model with apriori association rule and particle swarm optimization. *Security and Communication Networks*. https://doi.org/10.1155/2019/2850932.

Ahmad, P., Vincent Abbott, P., Khursheed Alam, M., & Ahmed Asif, J. (2019). A bibliometric analysis of the top 50 most cited articles published in the Dental Traumatology. *Dental Traumatology*. https://doi.org/10.1111/edt.12534.

Akour, M., Alsmadi, I., & Alazab, M. (2017). The malware detection challenge of accuracy. In *2016 2nd international conference on open source software computing, OSSCOM 2016*. https://doi.org/10.1109/OSSCOM.2016.7863750

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers and Security, 74,* 323–339. https://doi.org/10.1016/j.cose.2017.09.011.

Ali, W. (2019). Hybrid intelligent android malware detection using evolving support vector machine based on genetic algorithm and particle swarm. *Optimization, 19*(9), 15–28.

Almin, S. B., & Chatterjee, M. (2015). A novel approach to detect Android malware. *Procedia Computer Science, 45*(C), 407–417. https://doi.org/10.1016/j.procs.2015.03.170.

Amin, M., Tanveer, T. A., Tehseen, M., Khan, M., Khan, F. A., & Anwar, S. (2020). Static malware detection and attribution in android byte-code through an end-to-end deep system. *Future Generation Computer Systems, 102,* 112–126. https://doi.org/10.1016/j.future.2019.07.070.

An, N., Duff, A., Naik, G., Faloutsos, M., Weber, S., & Mancoridis, S. (2018). Behavioral anomaly detection of malware on home routers. In *Proceedings of the 2017 12th international conference on malicious and unwanted software, Malware 2017*, *2018-Janua* (pp. 47–54). https://doi.org/10.1109/Malware.2017.8323956

Arabo, A., & Pranggono, B. (2013). Mobile malware and smart device security: Trends, challenges and solutions. In *Proceedings—19th international conference on control systems and computer science, CSCS 2013* (pp. 526–531). https://doi.org/10.1109/CSCS.2013.27

Arzt, S., Rasthofer, S., Fritz, C., Bodden, E., Bartel, A., Klein, J., et al. (2014). FlowDroid: precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. *ACM Siglan Notices, 49*(6), 259–269. https://doi.org/10.1145/2666356.2594299.

Aung, Z., & Zaw, W. (2013). Permission-based android malware detection. *International Journal of Scientific & Technology Research, 2*(3), 228–234.

B, L. W. (2018). *Security with intelligent computing and big-data services* (Vol. 733). Berlin: Springer International Publishing. https://doi.org/10.1007/978-3-319-76451-1.

Baker, H. K., Kumar, S., & Pattnaik, D. (2019). Twenty-five years of Review of Financial Economics: A bibliometric overview. *Review of Financial Economics*. https://doi.org/10.1002/rfe.1095.

Basu, K., Krishnamurthy, P., Khorrami, F., & Karri, R. (2019). A theoretical study of hardware performance counters-based malware detection. *IEEE Transactions on Information Forensics and Security, 15*(c), 512–525. https://doi.org/10.1109/tifs.2019.2924549.

Belaoued, M., Boukellal, A., Koalal, M. A., Derhab, A., Mazouzi, S., & Khan, F. A. (2019). Combined dynamic multi-feature and rule-based behavior for accurate malware detection. *International Journal of Distributed Sensor Networks*. https://doi.org/10.1177/1550147719889907.

Besharati, E., Naderan, M., & Namjoo, E. (2018). LR-HIDS: logistic regression host-based intrusion detection system for cloud environments. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-018-1093-8.

Blanco-Mesa, F., Merigó, J. M., & Gil-Lafuente, A. M. (2017). Fuzzy decision making: A bibliometric-based review. *Journal of Intelligent and Fuzzy Systems, 32*(3), 2033–2050. https://doi.org/10.3233/JIFS-161640.

Bonilla, C. A., Merigó, J. M., & Torres-Abad, C. (2015). Economics in Latin America: A bibliometric analysis. *Scientometrics, 105*(2), 1239–1252. https://doi.org/10.1007/s11192-015-1747-7.

Chebyshev, V., Sinitsyn, F., Parinov, D., Larin, B., Kupreev, O., & Lopatin, E. (2019). *IT threat evolution Q2 2019*. Statistics. Karpersky. https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/. Accessed 3 Mar 2020.

Chen, D., Zhang, R., Zhao, H., & Feng, J. (2019). A bibliometric analysis of the development of ICD-11 in medical informatics. *Journal of Healthcare Engineering*. https://doi.org/10.1155/2019/1649363.

Chen, H. T., & Li, X. (2017). The contribution of mobile social media to social capital and psychological well-being: Examining the role of communicative use, friending and self-disclosure. *Computers in Human Behavior, 75,* 958–965. https://doi.org/10.1016/j.chb.2017.06.011.

Computer Hope. (2019). *Computer vs. smartphone*. Computer Hope. https://www.computerhope.com/issues/ch001398.htm. Accessed 3 Mar 2020.

Counterpoint. (2019). *Global smartphone market share: By quarter*. Counterpoint. https://www.counterpointresearch.com/global-smartphone-share/. Accessed 3 Mar 2020.

Cyber Security in Parallel and Distributed Computing. (2019). *Cyber Security in Parallel and Distributed Computing*. https://doi.org/10.1002/9781119488330

Daimi, K. (2017). *Computer and network security essentials* (pp. 1–618). Berlin: Springer. https://doi.org/10.1007/978-3-319-58424-9.

Davi, L., Dmitrienko, A., Sadeghi, A.-R., & Winandy, M. (2011). Privilege escalation attacks on android. In I. Burmester, M. Tsudik, G. Magliveras, & S. Ilic (Eds.), *Information security* (Vol. 6531, p. 346+). Berlin: Springer.

De Lorenzo, A., Martinelli, F., Medvet, E., Mercaldo, F., & Santone, A. (2020). Visualizing the outcome of dynamic analysis of Android malware with VizMal. *Journal of Information Security and Applications, 50,* 102423. https://doi.org/10.1016/j.jisa.2019.102423.

Deshpande, P., Sharma, S. C., Peddoju, S. K., & Junaid, S. (2018). HIDS: A host based intrusion detection system for cloud computing environment. *International Journal of Systems Assurance Engineering and Management, 9*(3), 567–576. https://doi.org/10.1007/s13198-014-0277-7.

Dobran, B. (2019). *27 terrifying ransomware statistics & facts you need to read*. PhoenixNap. https://phoenixnap.com/blog/ransomware-statistics-facts. Accessed 3 Mar 2020.

Dockrill, P. (2018). China just overtook the US in scientific output for the first time. Sciencealert. https://www.sciencealert.com/china-just-overtook-us-in-scientific-output-first-time-published-research. Accessed 3 Mar 2020.

Ellegaard, O., & Wallin, J. A. (2015). The bibliometric analysis of scholarly production: How great is the impact? *Scientometrics, 105*(3), 1809–1831. https://doi.org/10.1007/s11192-015-1645-z.

Enago Academy. (2018). *China overtakes U.S. with the highest number of scientific publications*. Enago Academy. https://www.enago.com/academy/china-overtakes-us-with-highest-number-of-scientific-publications/. Accessed 3 Mar 2020.

Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M. (2014). Android security: A survey of issues, malware penetration, and defenses. *IEEE Communications Surveys and Tutorials, 17*(2), 998–1022. https://doi.org/10.1109/COMST.2014.2386139.

Feizollah, A., Anuar, N. B., Salleh, R., Suarez-Tangil, G., & Furnell, S. (2017). AndroDialysis: Analysis of android intent effectiveness in malware detection. *Computers and Security, 65,* 121–134. https://doi.org/10.1016/j.cose.2016.11.007.

Feizollah, A., Anuar, N. B., Salleh, R., & Wahab, A. W. A. (2015). A review on feature selection in mobile malware detection. *Digital Investigation, 13,* 22–37. https://doi.org/10.1016/j.diin.2015.02.001.

Feizollah, A., Shamshirband, S., & Anuar, N. B. (2013). Anomaly detection using cooperative fuzzy logic controller. *Frontiers of Information Technology & Electronic Engineering*. https://doi.org/10.1631/fitee.1601491.

Feng, Y., Anand, S., Dillig, I., & Aiken, A. (2014). Apposcopy: Semantics-based detection of android malware through static analysis. In *22ND ACM SIGSOFT international symposium on the foundations of software engineering (FSE 2014)* (pp. 576–587). New York, NY: Assoc Computing Machinery. https://doi.org/10.1145/2635868.2635869

Firdaus, A., Razak, M. F. A., Feizollah, A., Hashem, I. A. T., Hazim, M., & Anuar, N. B. (2019). *The rise of "blockchain": Bibliometric analysis of blockchain study. Scientometrics* (Vol. 120). Berlin: Springer International Publishing. https://doi.org/10.1007/s11192-019-03170-4.

Galetsi, P., & Katsaliaki, K. (2019). Review article big data analytics in health: An overview and bibliometric study of research activity. *Health Information & Libraries Journal*. https://doi.org/10.1111/hir.12286.

Garg, S., Kaur, K., Batra, S., Kaddoum, G., Kumar, N., & Boukerche, A. (2020). A multi-stage anomaly detection scheme for augmenting the security in IoT-enabled applications. *Future Generation Computer Systems, 104,* 105–118. https://doi.org/10.1016/j.future.2019.09.038.

Gautam, P., Maheshwari, S., Kaushal-Deep, S. M., Bhat, A. R., & Jaggi, C. K. (2020). COVID-19: A bibliometric analysis and insights. *International Journal of Mathematical, Engineering and Management Sciences, 5*(6), 1156–1169. https://doi.org/10.33889/IJMEMS.2020.5.6.088.

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers and Security, 73,* 519–544. https://doi.org/10.1016/j.cose.2017.12.006.

Gorla, A., Tavecchia, I., Gross, F., & Zeller, A. (2014). Checking app behavior against app descriptions. In A. Jalote, P. Briand, & L. VanderHoek (Eds.), *36th international conference on software engineering (ICSE 2014)* (pp. 1025–1035). New York, NY: Assoc Computing Machinery. https://doi.org/10.1145/2568225.2568276.

Guanghui, S. (2020). *Thiết kế và triển khai hệ thống quản lý thể thao trường học dựa trên WEB. Springer Nature Thụy Sĩ AG 2020*. Springer International Publishing. https://doi.org/10.1007/978-3-030-15235-2

Haider, W., Creech, G., Xie, Y., & Hu, J. (2016). Windows based data sets for evaluation of robustness of Host based Intrusion Detection Systems (IDS) to zero-day and stealth attacks. *Future Internet, 8*(3), 29. https://doi.org/10.3390/fi8030029.

Ham, H.-S., Kim, H.-H., Kim, M.-S., & Choi, M.-J. (2014). Linear SVM-based android malware detection for reliable IoT services. *Journal of Applied Mathematics*. https://doi.org/10.1155/2014/594501.

Hu, X. L., Zhang, L. C., & Wang, Z. X. (2018). An adaptive smartphone anomaly detection model based on data mining. *Eurasip Journal on Wireless Communications and Networking, 2018*(1), 1–10. https://doi.org/10.1186/s13638-018-1158-6.

Huda, S., Islam, R., Abawajy, J., Yearwood, J., Hassan, M. M., & Fortino, G. (2018). A hybrid-multi filter-wrapper framework to identify run-time behaviour for fast malware detection. *Future Generation Computer Systems, 83,* 193–207. https://doi.org/10.1016/j.future.2017.12.037.

International Center. (2019). Research in China. International Center. https://international.uky.edu/OCI/Faculty/Research. Accessed 3 Mar 2020.

Iwami, S., Ojala, A., Watanabe, C., & Neittaanmäki, P. (2019). A bibliometric approach to finding fields that co-evolved with information technology. *Scientometrics*. https://doi.org/10.1007/s11192-019-03284-9.

Johnson, A. L. (2016). IoT devices being increasingly used for DDoS attacks. Broadcom. https://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks. Accessed 3 Mar 2020.

Jose, S., Malathi, D., Reddy, B., & Jayaseeli, D. (2018). A survey on anomaly based host intrusion detection system. *Journal of Physics: Conference Series, 1000*(1), 012049. https://doi.org/10.1088/1742-6596/1000/1/012049.

Kamesh, H., & Sakthi Priya, N. (2012). A survey of cyber crimes Yanping. *Security and Communication Networks, 5,* 422–437. https://doi.org/10.1002/sec.

Kim, T., Kang, B., Rho, M., Sezer, S., & Im, E. G. (2019). A multimodal deep learning method for android malware detection using various features. *IEEE Transactions on Information Forensics and Security, 14*(3), 773–788. https://doi.org/10.1109/TIFS.2018.2866319.

Koucham, O., Rachidi, T., & Assem, N. (2015). Host intrusion detection using system call argument-based clustering combined with Bayesian classification. In *IntelliSys 2015—Proceedings of 2015 SAI intelligent systems conference* (pp. 1010–1016). https://doi.org/10.1109/IntelliSys.2015.7361267

Kuntz, M., Tong, Y., & Lovaas, P. (2017). Challenges and strategies for malware analysis for incident response and prevention, *17*, 68–71. http://www.albany.edu/iasymposium/proceedings/2017/Challenges-P13.pdf

Lanet, J., Eds, C. T., Conference, I., & Hutchison, D. (2018). *For Information technology*. Berlin: Springer International Publishing. https://doi.org/10.1007/978-3-030-12942-2.

Li, J., Sun, L., Yan, Q., Li, Z., Srisa-An, W., & Ye, H. (2018). Significant permission identification for machine-learning-based android malware detection. *IEEE Transactions on Industrial Informatics, 14*(7), 3216–3225. https://doi.org/10.1109/TII.2017.2789219.

Liang, J., Chen, J., Zhu, Y., & Yu, R. (2019). A novel intrusion detection system for vehicular ad hoc networks (VANETs) based on differences of traffic flow and position. *Applied Soft Computing Journal, 75,* 712–727. https://doi.org/10.1016/j.asoc.2018.12.001.

Library. (2019). *Measuring research impact*. University of Leeds. https://library.leeds.ac.uk/info/1406/researcher_support/17/measuring_research_impact. Accessed 3 Mar 2020.

Library, U. (2020). *Research methodologies guide*. IOWA STATE UNIVERSITY. https://instr.iastate.libguides.com/researchmethods. Accessed 3 Mar 2020.

Ljubas, Z. (2020). *IT specialists warn of malware increase during COVID-19*. OCCRP. https://www.occrp.org/en/daily/12509-it-specialists-warn-of-malware-increase-during-covid-19. Accessed 8 Sept 2020.

Lookout. (2019). *What is a mobile threat?* Lookout. https://www.lookout.com/know-your-mobile/what-is-a-mobile-threat. Accessed 3 Mar 2020.

Lopes, J., Serrão, C., Nunes, L., Almeida, A., & Oliveira, J. (2019). Overview of machine learning methods for Android malware identification. In *7th international symposium on digital forensics and security, ISDFS 2019* (pp. 1–6). https://doi.org/10.1109/ISDFS.2019.8757523

Lu, C., Li, X., & Yang, K. (2019). Trends in shared decision-making studies from 2009 to 2018: A bibliometric analysis. *Frontiers in Public Health, 7,* 1–9. https://doi.org/10.3389/fpubh.2019.00384.

Luo, J., Han, H., Jia, F., & Dong, H. (2020). Agricultural Co-operatives in the western world: A bibliometric analysis. *Journal of Cleaner Production, 273,* 122945. https://doi.org/10.1016/j.jclepro.2020.122945.

Macmanus, R. (2012). *The future of connected cars: What audi is driving towards*. Readwrite. https://readwrite.com/2012/04/17/the_future_of_connected_cars_audi/. Accessed 3 Mar 2020.

Magdum, M. (2015). Permission based mobile malware detection system using machine learning. *Techniques, 14*(6), 6170–6174.

Martín, I., Hernández, J. A., & de los Santos, S. (2019). Machine-learning based analysis and classification of Android malware signatures. *Future Generation Computer Systems, 97,* 295–305. https://doi.org/10.1016/j.future.2019.03.006.

Mas'Ud, M. Z., Sahib, S., Abdollah, M. F., Selamat, S. R., & Yusof, R. (2014a). Analysis of features selection and machine learning classifier in android malware detection. In *ICISA 2014—2014 5th international conference on information science and applications*. https://doi.org/10.1109/ICISA.2014.6847364

Mas'ud, M. Z., Sahib, S. S., Abdollah, M. F., Selamat, S. R., & Yusof, R. (2014b). Android malware detection system classification. *Research Journal of Information Technology, 6*(4), 325–341. https://doi.org/10.3923/rjit.2014.325.341.

Mcafee. (2019a). *Ransomware attacks grew by 118%, new ransomware families were detected, and threat actors used innovative techniques*. Mcafee. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf. Accessed 3 Mar 2020.

McAfee. (2019b). *Mobile malware continues to increase in complexity and scope*. Mcafee. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf. Accessed 3 Mar 2020.

Merigó, J. M., Gil-Lafuente, A. M., & Yager, R. R. (2015). An overview of fuzzy research with bibliometric indicators. *Applied Soft Computing Journal, 27,* 420–433. https://doi.org/10.1016/j.asoc.2014.10.035.

Merigó, J. M., & Yang, J. B. (2017). Accounting Research: A Bibliometric Analysis. *Australian Accounting Review, 27*(1), 71–100. https://doi.org/10.1111/auar.12109.

Mobliciti. (2020). *Current trends in android mobile malware*. Mobliciti. https://mobliciti.com/current-trends-android-mobile-malware/. Accessed 3 Mar 2020.

Moon, D., Pan, S. B., & Kim, I. (2016). Host-based intrusion detection system for secure human-centric computing. *Journal of Supercomputing, 72*(7), 2520–2536. https://doi.org/10.1007/s11227-015-1506-9.

Moran, D. (2020). *Android malware takes advantage of Covid-19*. buguroo. https://www.buguroo.com/en/labs/android-malware-takes-advantage-of-covid-19. Accessed 2 Sept 2020.

Naga Malleswari, D., Dhavalya, A., Divya Sai, V., & Srikanth, K. (2017). A detailed study on risk assessment of mobile app permissions. *International Journal of Engineering Technology, 7*(1.1), 297.

Narudin, F. A., Feizollah, A., Anuar, N. B., & Gani, A. (2016). Evaluation of machine learning classifiers for mobile malware detection. *Soft Computing, 20*(1), 343–357. https://doi.org/10.1007/s00500-014-1511-6.

Niazi, R. A., & Faheem, Y. (2019). A Bayesian game-theoretic intrusion detection system for hypervisor-based software defined networks in smart grids. *IEEE Access, 7,* 88656–88672. https://doi.org/10.1109/ACCESS.2019.2924968.

Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic malware analysis in the modern era—A state of the art survey. *ACM Computing Surveys, 52*(5), 1–48. https://doi.org/10.1145/3329786.

Ospina-Mateus, H., Quintana Jiménez, L. A., Lopez-Valdes, F. J., & Salas-Navarro, K. (2019). Bibliometric analysis in motorcycle accident research: A global overview. *Scientometrics, 121*(2), 793–815. https://doi.org/10.1007/s11192-019-03234-5.

Palmer, D. (2019). *Mobile malware attacks are booming in 2019: These are the most common threats*. ZdNet. https://www.zdnet.com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats/. Accessed 3 Mar 2020.

Park, M., Oh, H., & Lee, K. (2019). Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective. *Sensors (Switzerland), 19*(9), 2148. https://doi.org/10.3390/s19092148.

Peiravian, N., & Zhu, X. (2013). Machine learning for android malware detection using permission and API calls. In *2013 IEEE 25th international conference on tools with artificial intelligence (ICTAI)* (pp. 300–305). New York, NY: IEEE. https://doi.org/10.1109/ICTAI.2013.53

Potteti, S., & Parati, N. (2015). Design of intrusion detection system for internet of things based on improved BP neural network. *International Journal of Engineering and Computer Science, 4*(5), 12146–12151.

Prashar, A., & Sunder, M. V. (2019). A bibliometric and content analysis of sustainable development in small and medium-sized enterprises. *Journal of Cleaner Production, 245,* 118665. https://doi.org/10.1016/j.jclepro.2019.118665.

Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems, 97,* 887–909. https://doi.org/10.1016/j.future.2019.03.007.

Raparelli, E., & Bajocco, S. (2019). A bibliometric analysis on the use of unmanned aerial vehicles in agricultural and forestry studies. *International Journal of Remote Sensing, 40*(24), 9070–9083. https://doi.org/10.1080/01431161.2019.1569793.

Rastogi, V., Chen, Y., & Jiang, X. (2014). Catch me if you can: Evaluating android anti-malware against transformation attacks. *IEEE Transactions On Information Forensics And Security, 9*(1), 99–108. https://doi.org/10.1109/TIFS.2013.2290431.

Razak, M. F. A., Anuar, N. B., Salleh, R., & Firdaus, A. (2016). The rise of "malware": Bibliometric analysis of malware study. *Journal of Network and Computer Applications, 75,* 58–76. https://doi.org/10.1016/j.jnca.2016.08.022.

Razak, M. F. A., Anuar, N. B., Salleh, R., Firdaus, A., Faiz, M., & Alamri, H. S. (2019). "Less Give More": Evaluate and zoning Android applications. *Measurement: Journal of the International Measurement Confederation, 133,* 396–411. https://doi.org/10.1016/j.measurement.2018.10.034.

Rehman, Z. U., Khan, S. N., Muhammad, K., Lee, J. W., Lv, Z., Baik, S. W., et al. (2018). Machine learning-assisted signature and heuristic-based detection of malwares in Android devices. *Computers and Electrical Engineering, 69,* 828–841. https://doi.org/10.1016/j.compeleceng.2017.11.028.

Reuters, T. (2008). Whitepaper using bibliometrics. *Thomson Reuters*. https://doi.org/10.1097/NCN.0b013e31819ec9ac.

Sanders, A. (2019). *15 (CRAZY) malware and virus statistics, trends & facts 2020*. Safety Detectives. https://www.safetydetectives.com/blog/malware-statistics/. Accessed 3 Mar 2020.

Sanz, B., Santos, I., Laorden, C., Ugarte-Pedrero, X., Garcia Bringas, P., & Alvarez, G. (2013). PUMA: Permission usage to detect malware in android. In E. Herrero, A. Snasel, V. Abraham, A. Zelinka, I. Baruque, B. Quintian, H. Calvo, J. L. Sedano, & J. Corchado (Eds.), *International joint conference CISIS'12—ICEUTE'12—SOCO'12 Special Sessions* (Vol. 189, p. 289+). Berlin: Springer.

Seals, T. (2020). *Malicious Google web extensions harvest cryptowallet secrets*. Threat Post. https://threatpost.com/malicious-google-web-extensions-cryptowallet/154832/. Accessed 8 Sept 2020.

Security, S. (2020). *COVID-19 pandemic sparks 72% ransomware growth, mobile vulnerabilities grow 50%*. Cision. https://www.prnewswire.com/in/news-releases/covid-19-pandemic-sparks-72-ransomware-growth-mobile-vulnerabilities-grow-50--817268901.html. Accessed 8 Sept 2020.

Seo, S.-H., Gupta, A., Sallam, A. M., Bertino, E., & Yim, K. (2014a). Detecting mobile malware threats to homeland security through static analysis. *Journal Of Network And Computer Applications, 38*(SI), 43–53. https://doi.org/10.1016/j.jnca.2013.05.008.

Seo, S. H., Gupta, A., Sallam, A. M., Bertino, E., & Yim, K. (2014b). Detecting mobile malware threats to homeland security through static analysis. *Journal of Network and Computer Applications, 38*(1), 43–53. https://doi.org/10.1016/j.jnca.2013.05.008.

Shabtai, A., Tenenboim-Chekina, L., Mimran, D., Rokach, L., Shapira, B., & Elovici, Y. (2014a). Mobile malware detection through analysis of deviations in application network behavior. *Computers and Security, 43,* 1–18. https://doi.org/10.1016/j.cose.2014.02.009.

Shabtai, A., Tenenboim-Chekina, L., Mimran, D., Rokach, L., Shapira, B., & Elovici, Y. (2014b). Mobile malware detection through analysis of deviations in application network behavior. *Computers & Security, 43,* 1–18. https://doi.org/10.1016/j.cose.2014.02.009.

Shabtai, A., Kanonov, U., & Elovici, Y. (2010). Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method. *Journal of Systems and Software, 83*(8, SI), 1524–1537. https://doi.org/10.1016/j.jss.2010.03.046.

Shabtai, A., Kanonov, U., Elovici, Y., Glezer, C., & Weiss, Y. (2012). "Andromaly": A behavioral malware detection framework for android devices. *Journal of Intelligent Information Systems, 38*(1), 161–190. https://doi.org/10.1007/s10844-010-0148-x.

Shankar, D. S., Chung, P. J., Hannah, T., Dreher, N., Li, A. Y., Dai, J. B., et al. (2020). The effect of academic rank and years in practice on bibliometric profile growth rates among academic neurosurgeons in the New York metropolitan area. *Interdisciplinary Neurosurgery: Advanced Techniques and Case Management, 19,* 100615. https://doi.org/10.1016/j.inat.2019.100615.

Sharma, K., & Gupta, B. B. (2016). Multi-layer defense against malware attacks on smartphone Wi-Fi access channel. *Physics Procedia, 78,* 19–25. https://doi.org/10.1016/j.procs.2016.02.005.

Sharma, K., & Gupta, B. B. (2018a). Attack in smartphone Wi-Fi access channel: State of the art, current issues, and challenges. *Advances in Intelligent Systems and Computing, 638,* 555–561. https://doi.org/10.1007/978-981-10-6005-2_56.

Sharma, K., & Gupta, B. B. (2018b). Mitigation and risk factor analysis of android applications. *Computers and Electrical Engineering, 71*(March), 416–430. https://doi.org/10.1016/j.compeleceng.2018.08.003.

Sharma, K., & Gupta, B. B. (2019). Towards privacy risk analysis in android applications using machine learning approaches. *International Journal of E-Services and Mobile Applications, 11*(2), 1–21. https://doi.org/10.4018/IJESMA.2019040101.

Sheen, S., Anitha, R., & Natarajan, V. (2015). Android based malware detection using a multifeature collaborative decision fusion approach. *Neurocomputing, 151*(P2), 905–912. https://doi.org/10.1016/j.neucom.2014.10.004.

Shrivastava, G., & Kumar, P. (2017). Privacy analysis of android applications: State-of-art and literary assessment. *Scalable Computing, 18*(3), 243–252. https://doi.org/10.12694/scpe.v18i3.1304.

Shrivastava, G., & Kumar, P. (2019a). Intent and permission modeling for privacy leakage detection in android. *Energy Systems*. https://doi.org/10.1007/s12667-019-00359-7.

Shrivastava, G., & Kumar, P. (2019b). Android application behavioural analysis for data leakage. *Expert Systems*. https://doi.org/10.1111/exsy.12468.

Shrivastava, G., & Kumar, P. (2019c). SensDroid: Analysis for malicious activity risk of android application. *Multimedia Tools and Applications, 78*(24), 35713–35731. https://doi.org/10.1007/s11042-019-07899-1.

Shukla, N., Merigó, J. M., Lammers, T., & Miranda, L. (2020). Half a century of computer methods and programs in biomedicine: A bibliometric analysis from 1970 to 2017. *Computer Methods and Programs in Biomedicine, 183,* 105075. https://doi.org/10.1016/j.cmpb.2019.105075.

Singhal, S., Maheshwari, S., & Meena, M. (2019). *Recent findings in intelligent computing techniques* (Vol. 707, pp. 229–238). Berlin: Springer. https://doi.org/10.1007/978-981-10-8639-7.

Spring, T. (2019). *Biggest malware threats of 2019*. Threat Post. https://threatpost.com/biggest-malware-threats-of-2019/151423/. Accessed 3 Mar 2020.

Statista. (2019). *Number of smartphone users worldwide from 2016 to 2021*. Statista. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. Accessed 3 Mar 2020.

Suárez-Tangil, G., Dash, S. K., García-Teodoro, P., Camacho, J., & Cavallaro, L. (2018). Anomaly-based exploratory analysis and detection of exploits in android mediaserver. *IET Information Security, 12*(5), 1–10. https://doi.org/10.1049/iet-ifs.2017.0460.

Suarez-Tangil, G., Tapiador, J. E., Pens-Lopez, P., & Blasco, J. (2014). DENDROID: A text mining approach to analyzing and classifying code structures in Android malware families. *Expert System with Applications, 41*(4), 1104–1117. https://doi.org/10.1016/j.eswa.2013.07.106.

Subba, B., Biswas, S., & Karmakar, S. (2017). Host based intrusion detection system using frequency analysis of n-gram terms. In *IEEE Region 10 Annual International Conference, Proceedings/TENCON, 2017-Decem*, 2006–2011. https://doi.org/10.1109/TENCON.2017.8228190

Taheri, R., Ghahramani, M., Javidan, R., Shojafar, M., Pooranian, Z., & Conti, M. (2020). Similarity-based Android malware detection using Hamming distance of static binary features. *Future Generation Computer Systems, 105,* 230–247. https://doi.org/10.1016/j.future.2019.11.034.

Tahir, M., Li, M., Zheng, X., Carie, A., Jin, X., Azhar, M., et al. (2019). A novel network user behaviors and profile testing based on anomaly detection techniques. *International Journal of Advanced Computer Science and Applications, 10*(6), 305–324. https://doi.org/10.14569/ijacsa.2019.0100641.

Talal, M., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Alsalem, M. A., Albahri, A. S., et al. (2019). *Comprehensive review and analysis of anti-malware apps for smartphones. Telecommunication Systems* (Vol. 72). New York: Springer. https://doi.org/10.1007/s11235-019-00575-7.

Talha, K. A., Alper, D. I., & Aydin, C. (2015). APK Auditor: Permission-based Android malware detection system. *Digital Investigation, 13,* 1–14. https://doi.org/10.1016/j.diin.2015.01.001.

Tam, K., Feizollah, A., Anuar, N. B., Salleh, R., & Cavallaro, L. (2017). The evolution of android malware and android analysis techniques. *ACM Computing Surveys, 49*(4), 1–41. https://doi.org/10.1145/3017427.

The App Store Celebrates 10 Years and 2 Million Apps. (2018). Betacrash. http://betacrash.com/app-store/. Accessed 3 Mar 2020.

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers and Security, 70,* 376–391. https://doi.org/10.1016/j.cose.2017.07.003.

TMS. (2011). Executive summary. *Engineering Solutions for Sustainability, 23,* 1–5. https://doi.org/10.1002/9781118196823.ch1.

Venkatraman, S., Alazab, M., & Vinayakumar, R. (2019). A hybrid deep learning image-based analysis for effective malware detection. *Journal of Information Security and Applications, 47,* 377–389. https://doi.org/10.1016/j.jisa.2019.06.006.

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior, 101,* 286–296. https://doi.org/10.1016/j.chb.2019.07.034.

Wang, X., Yang, Y., & Zhu, S. (2018). Automated hybrid analysis of android malware through augmenting fuzzing with forced execution. *IEEE Transactions on Mobile Computing*. https://doi.org/10.1109/TMC.2018.2886881.

Wang, W., Wang, X., Feng, D., Liu, J., Han, Z., & Zhang, X. (2014). Exploring permission-induced risk in android applications for malicious application detection. *IEEE Transactions on Information Forensics and Security, 9*(11), 1869–1882. https://doi.org/10.1109/TIFS.2014.2353996.

Wazid, M., Zeadally, S., & Das, A. K. (2019). Mobile banking: Evolution and threats: Malware threats and security solutions. *IEEE Consumer Electronics Magazine, 8*(2), 56–60. https://doi.org/10.1109/MCE.2018.2881291.

Webofknowledge. (2018). *Web of science core collection indexes*. Clarivate Analytics. http://images.webofknowledge.com/WOKRS533JR18/help/WOS/hp_database.html. Accessed 3 Mar 2020.

Wei, F., Roy, S., Ou, X., & Robby. (2014). Amandroid: A precise and general inter-component data flow analysis framework for security vetting of android apps. In *CCS'14: Proceedings of The 21st ACM conference on computer and communications security* (pp. 1329–1341). New York, NY: Assoc Computing Machinery. https://doi.org/10.1145/2660267.2660357

Whittaker, Z. (2019). *A cryptocurrency stealing app found on Google Play was downloaded over a thousand times*. TC. https://techcrunch.com/2019/05/23/cryptocurrency-stealing-android-app/. Accessed 3 Mar 2020.

Whitwam, R. (2020). Android antivirus apps are useless — Here's what to do instead. ExtremeTech. https://www.extremetech.com/computing/104827-android-antivirus-apps-are-useless-heres-what-to-do-instead. Accessed 3 Mar 2020.

Wu, D.-J., Mao, C.-H., Wei, T.-E., Lee, H.-M., & Wu, K.-P. (2012). DroidMat: Android malware detection through manifest and API calls tracing. In *Proceedings of The 2012 7th Asia joint conference on information security (ASIAJCIS 2012)* (pp. 62–69). Los Alamitos, CA: IEEE Computer Soc. https://doi.org/10.1109/AsiaJCIS.2012.18

Wu, F., Xiao, L., & Zhu, J. (2019). Bayesian model updating method based android malware detection for IoT services. In *2019 15th international wireless communications and mobile computing conference, IWCMC 2019* (pp. 61–66). https://doi.org/10.1109/IWCMC.2019.8766754

Yang, A., Zhuansun, Y., Liu, C., Li, J., & Zhang, C. (2019). Design of intrusion detection system for internet of things based on improved BP neural network. *IEEE Access, 7,* 106043–106052. https://doi.org/10.1109/ACCESS.2019.2929919.

Yang, C., Xu, Z., Gu, G., Yegneswaran, V., & Porras, P. (2014). DroidMiner: Automated mining and characterization of fine-grained malicious behaviors in android applications. In J. Kutylowski & M. Vaidya (Eds.), *Computer Security—ESORICS 2014, PT I* (Vol. 8712, pp. 163–182). Cham: Springer Int Publishing Ag.

Yao, R. Q., Ren, C., Wang, J. N., Wu, G. S., Zhu, X. M., Xia, Z. F., & Yao, Y. M. (2020). Publication trends of research on sepsis and host immune response during 1999–2019: A 20-year bibliometric analysis. *International Journal of Biological Sciences, 16*(1), 27–37. https://doi.org/10.7150/ijbs.37496.

Ye, N., Kueh, T. B., Hou, L., Liu, Y., & Yu, H. (2020). A bibliometric analysis of corporate social responsibility in sustainable development. *Journal of Cleaner Production, 272,* 122679. https://doi.org/10.1016/j.jclepro.2020.122679.

Yerima, S. Y., Sezer, S., & McWilliams, G. (2014). Analysis of Bayesian classification-based approaches for Android malware detection. *IET Information Security, 8*(1), 25–36. https://doi.org/10.1049/iet-ifs.2013.0095.

Yerima, S. Y., Sezer, S., McWilliams, G., & Muttik, I. (2013). A New Android Malware Detection Approach Using Bayesian Classification. In H. Barolli, L. Xhafa, F. Takizawa, M. Enokido, & T. Hsu (Ed.), *27TH international conference on advanced information networking and applications (AINA)* (pp. 121–128). New York, NY: IEEE. https://doi.org/10.1109/AINA.2013.88

Yerima, S. Y., Sezer, S., & Muttik, I. (2015). High accuracy android malware detection using ensemble learning. *IET Information Security, 9*(6), 313–320. https://doi.org/10.1049/iet-ifs.2014.0099.

Yu, D., Li, D. F., Merigó, J. M., & Fang, L. (2016). Mapping development of linguistic decision making studies. *Journal of Intelligent and Fuzzy Systems, 30*(5), 2727–2736. https://doi.org/10.3233/IFS-152026.

Yu, L., Pan, Z., Liu, J., & Shen, Y. (2013). Android malware detection technology based on improved Bayesian classification. In *Proceedings—3rd international conference on instrumentation and measurement, computer, communication and control, IMCCC 2013*, (pp. 1338–1341). https://doi.org/10.1109/IMCCC.2013.297

Yuan, Z., Lu, Y., Wang, Z., & Xue, Y. (2014). Droid-Sec: Deep learning in android malware detection. *ACM SIGCOMM Computer Communication Review, 44*(4), 371–372. https://doi.org/10.1145/2740070.2631434.

Yuan, Z., Lu, Y., & Xue, Y. (2016). Droiddetector: Android malware characterization and detection using deep learning. *Tsinghua Science and Technology, 21*(1), 114–123. https://doi.org/10.1109/TST.2016.7399288.

Zhang, M., Duan, Y., Yin, H., & Zhao, Z. (2014). Semantics-aware android malware classification using weighted contextual API dependency graphs. In *Proceedings of The 21st ACM conference on computer and communications* (pp. 1105–1116). New York, NY: Assoc Computing Machinery. https://doi.org/10.1145/2660267.2660359

Zhang, Yi., & Chen, Y. (2020). Research trends and areas of focus on the Chinese Loess Plateau: A bibliometric analysis during 1991–2018. *CATENA, 194,* 104798. https://doi.org/10.1016/j.catena.2020.104798.

Zhang, Y., Pu, S., Lv, X., Gao, Y., & Ge, L. (2020). Global trends and prospects in microplastics research: A bibliometric analysis. *Journal of Hazardous Materials, 400,* 123110. https://doi.org/10.1016/j.jhazmat.2020.123110.

Zheng, M., Sun, M., & Lui, J. C. S. (2013). DroidAnalytics: A signature based analytic system to collect, extract, analyze and associate android malware. In *2013 12th IEEE international conference on trust, security and privacy in computing and communications (TRUSTCOM 2013)* (pp. 163–171). New York, NY: IEEE. https://doi.org/10.1109/TrustCom.2013.25

Zhou, Y., & Jiang, X. (2012). Dissecting android malware: Characterization and evolution. In *2012 IEEE symposium on security and privacy (SP)* (pp. 95–109). New York, NY: IEEE. https://doi.org/10.1109/SP.2012.16

Zhu, H. J., You, Z. H., Zhu, Z. X., Shi, W. L., Chen, X., & Cheng, L. (2018). DroidDet: Effective and robust detection of android malware using static analysis along with rotation forest model. *Neurocomputing, 272,* 638–646. https://doi.org/10.1016/j.neucom.2017.07.030.