Multimedia Tools and Applications (2023) 82:20269–20281
https://doi.org/10.1007/s11042-023-14400-6

The current state and future of mobile security in the light of the recent mobile security threat reports

Ahmet Cevahir Cinar[1] · Turkan Beyza Kara[1]

Received: 30 January 2022 / Revised: 6 May 2022 / Accepted: 22 January 2023 /
Published online: 30 January 2023

Abstract
Smartphones have become small computers that meet many of our needs, from e-mail and banking transactions to communication and social media use. In line with these attractive functions, the use of smartphones has greatly increased over the years. One of the most important features of these mobile devices is that they offer users many mobile applications that they can install. However, hacker attacks and the spread of malware have also increased. Today, current mobile malware detection and defense technologies are still inadequate. Mobile security is not only directly related to the operating system and used device but also related with communication over the internet, data encryption, data summarization, and users' privacy awareness. The main aim and contribution of this study are to collect the current state of mobile security and highlight the future of mobile security in light of the recent mobile security threat reports. The studies in the field of malware, attack types, and security vulnerabilities concerning the usage of smartphones were analyzed. The malware detection techniques were analyzed into two categories: signature-based and machine learning (behavior detection)-based techniques. Additionally, the current threats and prevention methods were described. Finally, a future direction is highlighted in the light of the current mobile security reports.

Keywords Mobile threat report · Mobile security · Smartphone security · Security · Mobile applications

1 Introduction

Today the market of smart phones, which we use like mobile phones, tends towards tremendous sustainable growth [16]. According to the International Data Corporation (IDC)

✉ Ahmet Cevahir Cinar
accinar@selcuk.edu.tr; ahmetcevahircinar@gmail.com

✉ Turkan Beyza Kara
218273001009@lisansustu.selcuk.edu.tr

[1] Department of Computer Engineering, Faculty of Technology, Selçuk University, Konya, Turkey

Worldwide Quarterly Mobile Phone Tracker, total shipment volumes of smartphones increased by 13.2% year-over-year, with the 2020 recovery continuing with 313.2 million device shipments in the second quarter of 2021 [33].

One of the biggest factors in the popularity of smartphone use is the increase in functionality and the decrease the costs. In addition to offering many connection options such as Bluetooth, Wi-Fi, GPS, the fact that smartphones allow third-party applications to be installed expands the functionality limit. These applications are officially distributed by online stores. There are Google Play Store for the Android operating system and Apple App Store for iOS.

Attractive features such as unlimited internet access, numerous application options have become opportunities for malware developers. According to Kaspersky Security Network, 9,599,519 malware, adware, and riskware attacks on mobile devices were blocked in the third quarter of 2021 [43]. There are several ways of malware infection. They can be transmitted through a multimedia messaging service (MMS) or an email. They can also pose threats by exploiting vulnerabilities in-network or mobile devices. Users are most affected by downloading applications that contain malicious code.

Since 2019, there have been significant changes in education and business life due to the COVID 19 pandemic. This process, where online work from home has increased, has also provided an opportunity for malicious attacks. Due to the increase in communication over the Internet, data encryption and security have gained more importance. In addition, the expansion of the digital world, and the increase in the size of multimedia contents, along with encryption and security operations, have brought to the fore effective and efficient data summarization. Current studies in the field of data encryption and summarization continue increasingly.

Koppanati and Kumar [23] developed a polynomial cohesion-based multimedia encryption technique (P-MEC) over the cloud. With this technique, which they developed by focusing on cubic and polynomial compatibility, they proved that multimedia data is better protected over the cloud than some existing models. Rayappan and Pandiyan [38] developed a lightweight Feistel structure-based substitution permutation crypto model to secure multimedia data on the cloud. They confirmed that this model, developed by leveraging the effectiveness of the block cipher approach, is suitable for secure multimedia data communication over the cloud. Since the model is resistant to different attack resistances, it can be used safely in an uncertain cloud environment. Jayapandian [20] proposed a method that provides the best encryption method to reduce the encoding and decoding time in multimedia data. This method proved to reduce the application time by more than 50%. It also provided the highest data security in multimedia data and reduce overall execution time in dynamic cloud tasks. Gupta et al. [17] proposed an advanced identity-based encryption approach that hides the identity of users using the Lagrange coefficient consisting of a polynomial interpolation function. They showed that this method takes less time in encryption and decryption compared to the competitive method. Kumar [25] has developed a method of generating event summaries in a cloud environment to help users access large volumes of video data effectively. It proved that the method with event summarization and event search outperformed the models with the best F-measure. Lalotra et al. [27] proposed a new method called iReTADS. With the summarization technique, they aimed to reduce network traffic and ensure network security through a real-time neural network. Experimental results showed that iReTADS is effective in monitoring network traffic and detecting anomalies. They also suggested that the developed method could also benefit efforts to control pandemics using medical datasets for smart healthy cities.

The main aim and contribution of this study are to collect the current state of mobile security and highlight the future of mobile security in light of the recent mobile security threat

reports. The studies in the field of malware, attack types, and security vulnerabilities concerning the usage of smartphones were analyzed. The malware detection techniques were analyzed into two categories: signature-based and machine learning (behavior detection)-based techniques. Additionally, the current threats and prevention methods were described. Finally, a future direction is highlighted in the light of the current mobile security reports.

The remainder of this paper is organized as follows: Types of malwares and types of malicious attacks and mobile vulnerabilities are explained in Sections 2 and 3, respectively. In Section 4, the security solutions to be taken against mobile malware, and threat detection techniques are reviewed. Finally, the paper is concluded by how security studies will lighten the future in Section 5.

2 Types of malwares

Program pieces written with the aim of stealing users' information and damaging the system by attacking them are called malicious programs. Malicious programs can be identified in two categories: threats that require host programs and threats that are independent of each other [10]. The first is a piece of program linked to an application or program. The other is an independent program run by the system.

In addition, mobile malware can be divided into three groups according to its behavior: propagation behavior, remote control behavior, and malicious attack behavior [46]. The propagation behavior refers to the access of the malware to the users, the remote-control behavior refers to the use of the remote server, and the attack behavior refers to the attacking of the users with different applications after infecting their devices.

Various types of mobile malware exist. Table 1 highlights the most common types of mobile malware with names and their descriptions.

Table 1 Typical malware apps

Name	Description
Virus	Viruses are programs. But they replicate themselves, infecting from one device to another.
Spyware	It is used for any software that monitors, collects, and sends personal information to third parties without the user's knowledge or consent.
Trojan	Trojans are sent via emails. Once activated, it saves the system information within itself or opens the infected computers to remote access and sends the information to another computer via the internet.
Rootkit	A rootkit is a computer program that infects the computer, itself among the processes, and provides full control of your computer remotely to malicious people, which is very difficult to detect.
Botnet	Botnets are malicious software used by cyber hackers for various tasks by installing illegal methods (such as fake Android applications) on technological products such as smartphones, tablets, computers without the consent of the user.
Ransomware	It is software that attackers use to encrypt their victims' files. It states that it transmits the password for a certain fee.
Adware	It can be defined as adware that runs in the background of the system and settles on computers and mobile devices, often without the consent of the victims.
RiskTool	RiskTool is an application that performs operations such as deletion, copying, modification, seizure of personal data on the mobile device without the consent of the victim and appears to be legal.

As previously mentioned, in the third quarter of 2021, 9,599,519 attacks on mobile devices were detected, including malware, adware, and riskware. Among all detected mobile threats, RiskTool applications constitute the largest share with a rate of 65.84%. Apart from that, 676,190 malware packages were detected. 12,097 of them are packaged mobile banking trojans, and 6.157 of them are packaged mobile ransomware trojans [43].

2.1 Popular malwares

The Android operating system is more exposed to malicious attacks due to the high number of users and is open source based. The Apple iOS platform, on the other hand, is less exposed to malicious threats than the Android platform. In this section, the most known malicious threats to smartphones are summarized and given in Table 2.

The HummingBad family was discovered by Check Point in February 2016. It secretly installs a rootkit on Android devices. It also earns advertising revenue with fake applications that look real. According to analysts' determination, it is estimated to generate $300,000 monthly income [30]. HummingBad was discovered by Check Point in 2016 [12]. It has reached more than 85 million downloads. Surveillance or Pegasus is spyware that affects all Wechat users that can infect Android and iOS operating systems from social media platforms. This malware takes control of the device to obtain sensitive information. The malicious app, called Surveillance or Pegasus, was discovered by Citizen Lab in 2016. It affected Android and iOS operating systems [2].

Swearing is a trojan discovered by Tencent Researchers in 2017 that steals personal and important data from victims, infects the Android operating system, and has over 100,000 downloads [39]. Gooligan was discovered by Check Point in 2016 [39]. It is a rootkit that infects Android operating systems and causes security weakness in more than 1 million Google accounts. FalseGuide was discovered by Check Point in 2016 [37]. Infecting Android and iOS operating systems, this malware places botnets on people's devices for malicious advertising purposes. Triada was discovered by Kaspersky and Check Point. Infecting Android

Table 2 Popular malwares

Name	Type	Discover Date
HummingBad	Rootkit	2016
Surveillance or Pegasus	Spyware	2016
Gooligan	Rootkit	2016
FalseGuide	Botnet	2016
Triada	Trojan	2016
Trickbot	Trojan	2016
Ztorg	Trojan	2016
DressCode	Botnet	2016
Godless	Rootkit	2016
Hiddad	Trojan	2017
Swearing	Trojan	2017
Bad Rabbit	Ransomware	2017
RedDrop	Spyware	2018
GandCrab	Ransomware	2019
njRAT	Trojan	2019
BlackShades	Trojan	2019
LightSpy	Trojan	2020
xHelper	Trojan	2020
Xafecopy	Trojan	2020

operating systems, this malware uses a backdoor to steal money from victims. A SMS trojan bypasses CAPTCHA and steals money [28].

Hiddad is one of the malwares discovered by Check Point and Kaspersky in 2017. It is a trojan used to gain access to confidential personal data. It is effective on Android operating systems. Ztorg is a trojan that attacks Android operating systems, discovered by Kaspersky in 2016. Like others, it steals user login information by installing fake apps via Google Play and other application markets. DressCode malware was discovered by Kaspersky in 2016. Infecting Android operating systems, this malware creates botnets for malicious attackers who create fake network traffic using IP addresses, allowing them to generate revenue.

Discovered in 2016, the Godless malware family silently installs itself on Android devices. Causes annoying ads and apps to get remote instructions and gain root privilege [31]. Discovered in 2017, the Bad Rabbit malware family is a ransomware-type threat that targets Android devices. Installed and deployed, this threat collects bitcoins from the victim in exchange for releasing resources [24]. Discovered by Wandera's security researcher in 2018, RedDrop malware is a family of spyware threats that target Android devices. It is a threat that can steal the victim's device information, files, images, and audio recordings [7]. Of the thousands of malware families discovered by G Data experts in 2019, the most popular is GandCrab, a ransomware-type malware with over 408,000 versions [4]. Malwares named njRAT and BlackShades, versions 208,000 and 193,000 respectively, both used by malware developers to gain administrative control of the victim's device, were discovered by G Data experts in 2019 [4].

In 2020, experts at TrendMicro found that Apple WebKit vulnerabilities were used for remote code execution. This malicious threat was a trojan named LightSpy, which was distributed using news portals such as COVID-19 update sites. It targeted iOS devices to steal personal information, take screenshots and identify nearby Wi-Fi networks [8]. One of the popular mobile malwares of 2020 is xHelper, which targets the Android platform. Discovered by Check Point, this malware can download other malicious apps, display ads, and reinstall itself when deleted [36]. One of the most popular malware families of 2020, identified by Check Point, is the Xafecopy trojan. Xafecopy disguises itself as useful apps, installing malware on the device. He clicks on web pages with Wireless Application Protocol (WAP) billing, a form of mobile payment, and reflects it on the victim's cell phone bill [36]. According to the 2021 report by Check Point experts, the most popular malware was Trickbot, infecting 4% of the world's organizations. TrickBot emerged in 2016 as a Trojan threat designed to trick financial services and online banking users [40].

3 Types of malicious attacks and mobile vulnerabilities

3.1 Types of malicious attacks

A malicious attack (threat) is an attempt to abuse and exploit another computer by various means. These are threats to access personal data without the victim's knowledge and to take control of the device.

There are three types of threats including phishing, social engineering, and MITM.

1. **Social engineering** is a type of threat made by malicious social engineers to obtain your personal information from you by imitating the script (prosecutor, police, banker). Social

engineering threats on smartphones often occur through advertising. Malware is often secretly embedded in the content of adware and can be run independently of the user.
2. **Phishing** apps are fake apps that pretend to be a real secure app on the user's smartphone, trying to get hold of a person's login password and other information.
3. A **man-in-the-middle attack (MITM)** is the eavesdropping of communication between two links to capture and manipulate packets on the network. With this attack, the connection can be interrupted, or misleading communication can be created.

3.2 Mobile vulnerabilities

Vulnerabilities in mobile devices are a flaw in the operating system that makes the device vulnerable to attack. There are various reasons why Android and iOS mobile devices become vulnerable to threats. In particular, the fact that the Android operating system is more exposed to attacks is due to the fact that it is an open-source operating system. Neglecting to make regular updates, installing applications from official application stores or third-party stores without checking their authenticity cause security vulnerabilities. Victims can still be attacked, even if downloaded from protected stores such as the Apple Store and Google Play, as malicious hackers can place threatening code on the cover of a real app.

In 2020, 18,353 vulnerabilities were identified in the Common Vulnerabilities and Exposures (CVE) list. These record numbers are nearly four years in a row, more than triple the five years ago [34]. According to the Synopsys Cybersecurity Research Center (CyRC) report, 97% of software and systems tested during 2020 were found to contain security vulnerabilities. Mobile devices are threatened by vulnerabilities in insecure data storage and communication. Of the vulnerabilities, 80% were related to insecure data storage and 53% were related to unsecured communication [1, 45].

4 Security solutions against mobile malware and threats

Today, with the increasing use of mobile devices, cybercriminals have begun to target mobile devices more than personal computers and laptops. A two-step method can be followed to protect mobile devices from malware and threats. First, preventive measures can be taken. Security measures should be taken to prevent attacks and malware infection on mobile devices. In the second stage, various tools can be used to detect the presence of malicious software.

The remainder of this section reviews techniques for detecting and blocking malware. It also offers some measures to minimize malware attacks.

4.1 Malware detection techniques

Techniques such as file access permission and sandboxing were applied to take security measures on Android and iOS mobile devices. However, they have been insufficient in preventing attacks that have recently increased and continue to increase.

Malicious attacks tripled from 2015, reaching over 8 million in 2016, causing more than $100 million in lost money worldwide [26]. In 2020, SonicWall Capture Labs threat researchers recorded 5.6 billion malware attacks. This figure is a huge decrease compared to the previous year. However, this situation cannot be seen as a success. Because, with many people

starting to work from home, cyber security providers are gradually losing the ability to monitor traffic and potential attacks. So this number could be much higher [15].

Researchers have divided malware detection techniques into two categories: signature-based and machine learning (behavior detection)-based techniques. The summary of the malware detection techniques is given in Table 3.

4.1.1 Signature based techniques

The signature-based technique is a technique for detecting and identifying certain patterns of malware, called signatures. The way of work this type of method is explained as follows: Generates a new signature by comparing a newly defined signature with existing signatures in the database. The downside of this technique is that if malware developers make minor changes to the new version of their app, the signature won't work. The comparison of the signature is made by overlapping.

Tchakounté et al. [47] developed an analysis tool called LimonDroid to identify malicious characters in Android apps. Using Yet Another Recursive/Ridiculous Acronym (YARA) [32] rules, this tool exposed malicious characters of Metasploit, Fake Apps, LeadBolt, Ransomware, RuMMS, Viking Horde, and XBot in scanned applications. Studies show that LimonDroid outperforms existing similarity-based solutions. It can also predict the class of an application with 97.82% accuracy. Dimolianis et al. [13] have presented an integrated scheme for signature-based traffic classification processing for DDoS protection. With this signature-based scheme, it outperformed traditional IP-based schemes in terms of malicious traffic categorization, cardinality of filtering rules, and packet processing efficiency in high-speed networks. The AMD framework, developed by Patil et al. [35], includes a VM operator that detects known malware with signature and anomaly detection techniques. The downside is that due to its distributed and dynamic nature, it includes security issues for cloud computing. VMs were over 96% successful in detecting malware. Thus, it secured the high-risk VMs of cloud computing. FOSS (Free and Open Source Software) performs a file system scan based on Nessus and YARA signatures developed by Jaramillo [19]. This application is developed against Mirai botnets, which are malware that includes DDoS attacks, damaging banking systems. Nessus is not open source and is low-cost. Savenko et al. [42] have done a study that generates virus signatures based on API call tracing. The recommended signature format for detecting malware allows distinguishing malicious applications from other applications by key

Table 3 Malware detection techniques

Signature-based techniques			Machine Learning-based techniques		
Name	Release Year	Reference	Name	Release Year	Reference
LimonDroid	2021	[47]	Chen et al.	2018	[9]
Dimolianis et al.	2021	[13]	Hatcher et al.	2016	[18]
The AMD framework	2020	[35]	Feizollah et al.	2013	[14]
FOSS	2018	[19]	ML-SMEPF	2021	[49]
Savenko et al.	2019	[42]	MLCD	2020	[29]
Venugopal and Hu	2018	[48]	IntruDTree	2020	[41]
SafeGuard	2017	[21]	Bosaeed et al.	2020	[5]
SensDroid	2019	[44]	AVIS	2018	[22]
			Arif et al.	2021	[3]

API calls. Up to 96.56% success was achieved in the trial results. Venugopal and Hu [48] have detailed a signature matching algorithm used in mobile device scanning. They developed their proposed signature-based malware detection method for low-memory mobile devices. This algorithm provides fast scanning and consumes less than 50% of memory compared to the Clam-AV scanner. Jeong et al. [21] presented a real-time malware detection software that named as SafeGuard. Shrivastava and Kumar [44] presented a Android Intent and permission based software that named as SensDroid.

4.1.2 Machine learning-based techniques

Machine learning (behavioral) based techniques are widely used in cyber security applications. Using this technique on a benign malware dataset, both unforeseen and known threats can be detected. Machine learning-based methods are preferred by many researchers in cyber security products, especially since they are more successful than signature-based methods in detecting zero-day attacks. In this section, we examine studies in which machine learning-based methods are used as a tool in malware analysis studies.

In their study of machine learning-based mobile malware detection using highly unstable network traffic, Chen et al. [9] confirmed that machine learning algorithms are effective in analyzing malicious mobile network traffic. Malicious mobile network traffic data is one of the well-known highly imbalanced datasets. However, they have shown that once the data imbalance reaches over 4000, no method can be effective on highly unstable problems. The proposed methods detect the malicious traffic flow in a very big benign traffic flow when the imbalance ratio is under 4000. Hatcher et al. [18] conducted mobile threat monitoring and detection studies using four machine learning methods (ZeroR, OneR, Naïve Bayes, and J48). As a result of the study, it was found that the best classifier could achieve 100% accuracy with a detection rate of 94.59%. Feizollah et al. [14] in their study comparing five types of machine learning classifiers (Naive Bayes, KNN, Decision Trees, MLP, and SVM) for anomaly-based mobile botnet detection, reached a detection rate of 99.94% with KNN. Wang et al. [49] have proposed Machine Learning-Assisted Secure Mobile Electronic PaymentFramework (ML-SMEPF) to detect malware, fraud, authentication issues in mobile transactions. They have proven the reliability of the framework in the simulation performed according to accuracy, safety, performance, and cost factor. Li et al. [29] highlighted the importance of mobile vehicle social networks (VSNs), which will provide a new method of code propagation with the evolution of 5G networks. They proposed the ‘‘Machine Learning based Code Dissemination by Selecting Reliability Mobile Vehicles in 5G Networks’’ (MLCD) to select lower-cost codes and code spreading tools with high reliability and coverage. In their study, they concluded that by comparing the MLCD scheme with other schemes, it can improve code propagation security by 83.6% and 18.86% with limited costs, and the coverage rate of updated information by 23.16% in 5G networks.

Sarker et al. [41] developed a machine learning-based cyber security attack detection model called IntruDTree. They tested the effectiveness of the model by conducting experiments on cyber security datasets. They analyzed the effectiveness of IntruDTree, a tree-based generalized intrusion detection model, by comparing it to traditional popular machine learning methods. They emphasized that the effectiveness of the model can be evaluated in IoT security services and cyber security in the future. Bosaeed et al. [5] have proposed a model on SMS Spam Detection and Classification System based on Fog Augmented Machine Learning. In this technique, in which they use three classification methods (Naïve Bayes (NB), Support

Vector Machine (SVM), and Naive Bayes Multinomial (NBM)), it detects spam, especially from outgoing SMS messages. As a result of their studies, they found that the PF5 filter and SVM had the best performance in SMS classification. Kim et al. [22] proposed a Vulnerability Identification System (AVIS) that can identify malicious applications in advance using the Naïve Bayes classification algorithm. Arif et al. [3] proposed a multi-criteria decision-making based mobile malware detection system using a risk-based fuzzy analytical hierarchy process approach to evaluate the Android mobile application.

4.2 Security measures to protect from malware and threats

Software vulnerabilities in mobile devices, vulnerabilities in wireless networks, security flaws caused by user errors, and security flaws in mobile applications are factors that attract malicious attackers. Users, application developers, network designers, and application market managers have responsibilities to prevent the transmission of malware and threats to mobile devices.

Smartphones are small computers. Users should protect their phones from fake and adware containing malware. They should use a good malware framework like a firewall and download apps (games, marketing, etc.) only from trusted app markets (Apple Store and Google Play Store, etc.). In addition, features such as WiFi or Bluetooth should not be left open if they are not in use, to protect against malware that can be transmitted by proximity contact with peer-to-peer communication methods.

There is heavy user activity on networks around the world. Users may have to share their personal data with the network service. Although their privacy policies are strongly defined and analyzed, users do not know how their information is managed by network providers and they use Facebook, Twitter, Instagram, etc. to benefit from their services. provide their information to service providers [11]. Due to the nature of information sharing and the need to process big data, including web data sources, privacy protection becomes more difficult [6]. Security control protocols may also be missing in this law. For all these reasons, users should be aware that their personal data may be exposed to malicious attacks while shopping online, browsing online sites, and during any transaction on the internet.

Network designers must protect network traffic from intruders such as attackers and opportunistic malware. For example, when the user connects to a free Wi-Fi, hackers may be listening to that data connection line and the user's personal data is in danger.

Application security is the precautions to be taken to avoid exposure to malicious attacks while developing applications and to prevent theft of important data in the application. In order to develop a secure application; During the planning, design, implementation, and testing phases, security studies should be carried out completely. Finally, after the application is released, the process should be followed, new security vulnerabilities should be detected, and updates should be made.

Server-side inspection processes have been developed to successfully test installed applications and detect malware. Administrators should implement well-defined security policies. For example, iPhone applications can only be downloaded from the App Store. In other words, applications that comply with Apple's security policies can be installed on iPhone devices.

5 Conclusion

While the number of smartphone usage continues to increase rapidly, especially the mobile usage areas have expanded with the impact of the COVID-19 epidemic in recent years.

Malware and threats are rapidly diversifying, renewing, and improving themselves. Mobile security is not only directly related to the operating system and used device but also related with communication over the internet, data encryption, data summarization, and users' privacy awareness.

In this paper, we first touched on malware and attack types, and security vulnerabilities. Then, current threat detection and prevention methods were deeply analyzed. Finally, we reviewed the ongoing threat detection and prevention efforts of developers in the mobile security space that were reported in recent mobile security threat reports.

While there are new methods in security studies related to mobile devices, malicious attackers also develop new methods in malware and threats. Security efforts in personal and corporate mobile devices need to be strengthened to protect against malicious attacks that continue with unpredictable growth.

Signature-based detection studies (cryptographic hash or package name) are used very often, but they are not successful enough. Malware and threats are constantly evolving and changing themselves to avoid detection by current security tests. Therefore, more machine learning algorithms should be used for detecting fake mobile applications and network monitoring in a timely manner. Testing for malware and threats should be performed dynamically using deep learning algorithms. For these tests to yield successful results, security companies must be more generous in making their malware datasets public. Otherwise, malware detection and recognition studies using smaller data samples may be insufficient.

Despite the increase in mobile malware and threats, corporate mobile usage has become widespread in recent years, with bring-your-own-device (BYOD) policies. This spread accelerated as people started working from home due to the COVID-19 outbreak. This creates new opportunities for malware developers. Organizations that must employ a mobile-friendly workforce need to increase the necessary cyber security measures both to protect the personal data security of the employees and to protect the information belonging to the sensitive organization.

In the light of the current studies, and the mobile security reports, the future of mobile security can be focused on these sub-research areas and topics:

a) New signature-based techniques powered with machine learning-based techniques can be proposed,
b) New machine learning-based techniques that especially work with imbalanced network traffic datasets can be produced,
c) New classification algorithms can be presented that detect the malicious flow,
d) The storage of the sensitive user data can be secured with new techniques,
e) The Android market rules can be redesigned similarly to iOS market rules.

Acknowledgements The authors wish to thank Scientific Research Projects Coordinatorship at Selcuk University and The Scientific and Technological Research Council of Turkey for their institutional supports.

Authors' contributions Ahmet Cevahir Cinar: Conceptualization, Methodology, Writing- Reviewing and Editing, Supervision.
Turkan Beyza Kara: Investigation, Writing- Original draft preparation.

Data availability Not applicable.

Code availability Not applicable.

Declarations

Conflicts of interest/Competing interests The authors have no conflicts of interest to declare that are relevant to the content of this article.

References

1. (CyRC) CRC (2021) 2021 software vulnerability snapshot. Synopsys. https://www.synopsys.com/software-integrity/resources/analyst-reports/software-vulnerability-trends.html?cmp=pr-sig&utm_medium=referral
2. Alvarez-Cedillo JA, Perez-Romero P, Hernandez-Bolaños M (2012) Bluetooth intrusion techniques. IRACST-International J Comput Sci Inform Technol Secur (IJCSITS) 2(1):208–215
3. Arif JM, Ab Razak MF, Mat SRT, Awang S, Ismail NSN, Firdaus A (2021) Android mobile malware detection using fuzzy AHP. J Inf Secur Appl 61:102929
4. Berghof T (2020) Malware Top 10 in 2019: attacks every few seconds. https://www.gdatasoftware.com/news/2020/01/35727-malware-top-10-in-2019-attacks-every-few-seconds
5. Bosaeed S, Katib I, Mehmood RA (2020) Fog-augmented machine learning based SMS spam detection and classification system. In: 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC). IEEE, pp 325–330
6. Breve B, Caruccio L, Cirillo S, Desiato D, Deufemia V, Polese G (2020) Enhancing user awareness during internet browsing. In: ITASEC, pp 71–81
7. Campbell N RedDrop: the blackmailing mobile malware family lurking in app stores. Wandera. https://www.wandera.com/blog/reddrop-malware/
8. Chebyshev V (2021) Mobile malware evolution 2020. https://securelist.com/mobile-malware-evolution-2020/101029/
9. Chen Z, Yan Q, Han H, Wang S, Peng L, Wang L, Yang B (2018) Machine learning based mobile malware detection using highly imbalanced network traffic. Inf Sci 433:346–364
10. Chen L, Xia C, Lei S, Wang T (2021) Detection, traceability, and propagation of mobile malware threats. IEEE Access 9:14576–14598
11. Cirillo S, Desiato D, Breve B (2019) CHRAVAT-chronology awareness visual analytic tool. In: 2019 23rd international conference information visualisation (IV). IEEE, pp 255–260
12. Das A, Khan HU (2016) Security behaviors of smartphone users. Inf Comput Secur 24(1):116–134
13. Dimolianis M, Pavlidis A, Maglaris V (2021) Signature-based traffic classification and mitigation for DDoS attacks using programmable network data planes. IEEE Access 9:113061–113076
14. Feizollah A, Anuar NB, Salleh R, Amalina F, Shamshirband S (2013) A study of machine learning classifiers for anomaly-based mobile botnet detection. Malaysian J Comput Sci 26(4):251–265
15. Grelg J (2021) Ransomware attempt volume sets record, reaches more than 300 million for first half of 2021: SonicWall. https://www.zdnet.com/article/ransomware-attack-volume-sets-record-reaches-more-than-300-million-for-first-half-of-2021-sonicwall/
16. Gupta BB, Yamaguchi S, Agrawal DP (2018) Advances in security and privacy of multimedia big data in mobile and cloud computing. Multimed Tools Appl 77(7):9203–9208
17. Gupta RK, Almuzaini KK, Pateriya R, Shah K, Shukla PK, Akwafo R (2022) An improved secure key generation using enhanced identity-based encryption for cloud computing in large-scale 5G. Wirel Commun Mob Comput 2022:14
18. Hatcher WG, Maloney D, Yu W (2016) Machine learning-based mobile threat monitoring and detection. In: 2016 IEEE 14th International Conference on Software Engineering Research, Management and Applications (SERA). IEEE, pp 67–73
19. Jaramillo LES (2018) Malware detection and mitigation techniques: lessons learned from Mirai DDOS attack. J Inf Syst Eng Manag 3(3):19
20. Jayapandian N (2021) Cloud dynamic scheduling for Multimedia Data encryption using Tabu Search Algorithm. Wirel Pers Commun 120(3):2427–2447
21. Jeong ES, Kim IS, Lee DH (2017) SafeGuard: a behavior based real-time malware detection scheme for mobile multimedia applications in android platform. Multimed Tools Appl 76(17):18153–18173
22. Kim H, Cho T, Ahn G-J, Yi JH (2018) Risk assessment of mobile applications based on machine learned malware dataset. Multimed Tools Appl 77(4):5027–5042

23. Koppanati RK, Kumar K (2020) P-MEC: polynomial congruence-based Multimedia encryption technique over cloud. IEEE Consum Electron Mag 10(5):41–46
24. Kumar M (2017) Bad rabbit: new ransomware attack rapidly spreading across Europe. https://thehackernews.com/2017/10/bad-rabbit-ransomware-attack.html
25. Kumar K (2021) Text query based summarized event searching interface system using deep learning over cloud. Multimed Tools Appl 80(7):11079–11094
26. lab. K (2016) Mobile malware evolution 2016. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180734/Mobile_report_2016.pdf
27. Lalotra GS, Kumar V, Bhatt A, Chen T, Mahmud M (2022) iReTADS: an intelligent real-time anomaly detection system for cloud communications using temporal data summarization and neural network. Secur Commun Netw 2022
28. Lee K-C, Hsieh C-H, Wei L-J, Mao C-H, Dai J-H, Kuang Y-T (2017) Sec-Buzzer: cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation. Soft Comput 21(11): 2883–2896
29. Li T, Zhao M, Wong KKL (2020) Machine learning based code dissemination by selection of reliability mobile vehicles in 5G networks. Comput Commun 152:109–118
30. Martinelli F, Mercaldo F, Nardone V, Santone A, Vaglini G (2020) Model checking and machine learning techniques for HummingBad mobile malware detection and mitigation. Simul Model Pract Theory 105: 102169
31. Micro T, Research N and Perspectives (2016) 'GODLESS' mobile malware roots devices. https://www.trendmicro.com/en_us/research/16/f/godless-mobile-malware-uses-multiple-exploits-root-devices.html#:~:text=We%20came%20across%20Godless%20(detected,of%20Android%20devices%20running%20today
32. Naik N, Jenkins P, Cooke R, Gillett J, Jin Y (2020) Evaluating automatically generated YARA rules and enhancing their effectiveness. In: 2020 IEEE Symposium Series on Computational Intelligence (SSCI). IEEE, pp 1146–1153
33. Needham M (2021) The global smartphone market grew 13.2% in the second quarter despite supply concerns and vendor shakeups, according to IDC. IDC. https://www.idc.com/getdoc.jsp?containerId=prUS48120021
34. NIST CVSS severity distribution over time. Information Technology Laboratory. https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time
35. Patil R, Dudeja H, Modi C (2020) Designing in-VM-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing. Int J Inf Secur 19(2):147–162
36. Point C September 2020's most wanted malware: new info-stealing valak variant enters top 10 malware list for first time. Check Point Software Technologies ltd. https://blog.checkpoint.com/2020/10/07/september-2020s-most-wanted-malware-new-info-stealing-valak-variant-enters-top-10-malware-list-for-first-time/
37. Point C https://www.checkpoint.com/press/2017/ransomware-doubled-second-half-2016-says-check-point/
38. Rayappan D, Pandiyan M (2021) Lightweight Feistel structure based hybrid-crypto model for multimedia data security over uncertain cloud environment. Wirel Netw 27(2):981–999
39. Sadiku M, Shadare A, Musa S (2016) Social engineering: an introducction. J Sci Eng Res 3:64–66
40. SAN CARLOS C (2021) September 2021's most wanted malware: trickbot once again tops the list. Check Point Software Technologies Ltd. https://www.checkpoint.com/press/2021/september-2021s-most-wanted-malware-trickbot-once-again-tops-the-list/
41. Sarker IH, Abushark YB, Alsolami F, Khan AI (2020) Intrudtree: a machine learning based cyber security intrusion detection model. Symmetry 12(5):754
42. Savenko O, Nicheporuk A, Hurman I, Lysenko S (2019) Dynamic signature-based Malware detection technique based on API call tracing. In: ICTERI workshops, pp 633–643
43. Shishkova T (2021) IT threat evolution in Q3 2021. Mobile statistics. https://securelist.com/it-threat-evolution-in-q3-2021-mobile-statistics/105020/
44. Shrivastava G, Kumar P (2019) SensDroid: analysis for malicious activity risk of android application. Multimed Tools Appl 78(24):35713–35731
45. Staff V (2021) Report: applications and critical data vulnerable to attack. VentureBeat. https://venturebeat.com/2021/11/26/report-applications-and-critical-data-vulnerable-to-attack/
46. Sui A-F, Guo (2012) T A behavior analysis based mobile malware defense system. In: 2012 6th international conference on signal processing and communication systems. IEEE, pp 1–6
47. Tchakounté F, Ngassi RCN, Kamla VC, Udagepola KP (2021) LimonDroid: a system coupling three signature-based schemes for profiling android malware. Iran J Comput Sci 4(2):95–114
48. Venugopal D, Hu G (2008) Efficient signature based malware detection on mobile devices. Mob Inf Syst 4(1):33–49

49. Wang F, Yang N, Shakeel PM, Saravanan V (2021) Machine learning for mobile network payment security evaluation system. Trans Emerg Telecommun Technol:e4226