MOBILE DEVICES AND CYBERSECURITY ISSUES AUTHENTICATION TECHNIQUES WITH MACHINE LEARNING

Eman Abdullah Aldakheel, College of Computer and Information Sciences Princess Nourah Bint Abdulrahman University
Mohammed Zakariah, College of Computer and Information Sciences King Saud University

ABSTRACT

Cybersecurity is the most important and hot research topic, especially at this time. As people are getting more dependent on digital systems and critical and sensitive information's are stored on these digital devices. There is an advantage of using these devices and gadgets. Still, at the same time, there is a risk of getting attacks on these sensitive files, be it money or essential transaction information for business dealings like customer information for a business. In this study, various security threats have been discussed, mainly for mobile devices. First, the harmful effects of using mobile phones concerning the attacks on these devices have been discussed. After that, authentication techniques are discussed, which show the various methods being applied to safeguard the mobile devices from intruders for malware attacks. There are four authentication techniques discussed in this work: authentication based on information, authentication based on biometrics, authentication based on behavioral, and authentication based on double factor. Each authentication technique is discussed with its advantages and disadvantages. Finally, the importance of machine learning for the detection of malware is discussed. There are various proposed techniques available that are designed using machine learning to fight malware attacks. Some of them are discussed here, which would help a new researcher in getting the proper research direction. At the end, recommendations are listed which can help to save the mobile device users from any attacks. These recommendations are categorized for users, researchers and government authorities.

Keywords: Cybersecurity, Malware, Mobile Devices, Authentication, Machine Learning

INTRODUCTION

In the last 100 years, the most significant development that took place technically is the invention of the internet. It is most beneficial because the devices are developed which could be connected based on the availability of the internet. The creation of the internet has given birth to many electronic and communication devices which are efficiently used for communication. In all those devices, smartphones are the number one in the list of devices being developed. Since the outcome of the internet, there is a demand of devices which could be interconnected for various functionality and different kind of users. But these smart devices are very much vulnerable among all the devices which exist in this ecosystem. However, these vulnerabilities and introduced cybersecurity concepts to tackle the threats. In an IoT scenario where every component is can produce and consume services. Based on the past research, it has come to know that on average, each person owns almost three inter-connected smart devices like smartphones and tablets are some of them (Cyber Security, 2011). So, this is leading to the ubiquity of smartphones, and this is the cause for the evolution of computing platforms. Also, the availability of powerful processors which are built inside the smart devices is making them more suitable for the inclusion of botnets. Mobile devices with botnet are considered as a kind of smart device which is compromised for attacks. These devices are controlled remotely by bot-

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

masters through a channel called command-and-control (C&C). Mobile botnets are a little different from PC-botnets. Mobile botnets are considered less threatful as compared to PC-based botnets for security attacks. Smart devices are very much in use because of their ability of enhanced computing and access to the internet more efficiently. As the usage is so intensive, so also the risk of getting attacks on these devices as sensitive a piece of private information is stored in large quantities. This information could be personal as most of the payments are made using smart devices for other sensitive transactions. As the usage of these devices is very wider and the open-source Android is applied as a third-party application, these things made when they are made available to the public would invite n creators to enter these devices and attack the information. So, based on these constraints, it is predicted that smart devices would be a target soon for cybercrimes. The above-discussed issue could be properly supported by the statistics which show how vulnerable the smart devices are if it is measured with the scale of security and privacy. Society is changing drastically and is shifting to online systems and are broadly adopting digital technology in almost every aspect of life, be it entertainment or social interactions, business dealings, industries, etc. As people are shifting to digital technology at a big pace so also the crime is increasingly reported. If the statistics are seen for the recent years, as much as USD 6 trillion are affected by the cybercrimes, and it is rising consistently as reported by (Blumberg, 2011), and another study also supports this as the crimes are taking place conventionally for both number and revenue (Juniper, 2012). These cybercrimes are becoming more composite because of creating extra multi-stage attacks (Juniper, 2012). As said in this (O'Gorman, 2003), the cyber-attacks in 2018 with malicious packages which took place per day was around 9600. These kinds of malicious attacks lead to severe damage to financial losses, which reached USD one billion, as it was stolen from financial institutions over a span of two years around the world with the application of malware (Uellenbeck, 2013). Additionally, Kingsoft assessed around two to five million computers were attacked per day (Chiasson, 2007). In one study (Aviv, 2010), during 2018, around 1.5 trillion USD of cybercrimes affected the revenue, and the global cost was estimated to be around USD 6 trillion by 2021 (Song, 2001). The whole paper contents are shown in pictorial form in Fig. 1. Based on these statistics, it is understood that addressing these cybercrimes has become an urgent issue to be handle intelligently with the implementation of the latest technologies.

The main objective and contribution of this work can list as follows:

- In this study, various security threats have been discussed, mainly for mobile devices.
- The harmful effects of using mobile phones concerning the attacks on these devices have been discussed.
- Authentication techniques are discussed, which show the various methods being applied to safeguard the mobile devices from intruders for malware attacks.
- The importance of machine learning for the detection of malware. There are various proposed techniques available that are designed using machine learning to fight malware attacks.

FIGURE 1
MAJOR COMPONENTS OF THE PAPER

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

The rest of the paper is as follows: section 1 gives the complete introduction about the research field, section 2 discusses the Cybersecurity in Company Employee, section 3 describes the security threats on smart devices, section 4 discussed various authentication techniques, followed by section 5 discuss the machine learning for malware, and section 6 discussed few recommendations for smartphone users, researchers, and government authorities and section 7 has the conclusion and followed by the list of references.

Cybersecurity in Company Employee Perspective

The usage of mobile devices by the employees working in companies is continuously growing, and the reason for this is the change in technology and globalization and the growing expectations from them. Based on these issues, the employees very much prefer to use mobile devices, especially smartphones which would help them in adhere faster to innovations and provide the flexibility to work and get better quality outcomes by making efficient collaborations by communicating with experts across the borders (Miluzzo, 2012). As the employees are preferring the usage of mobile devices for their regular work but managing their data for security aspects is a regular challenge. It is a challenge because these employees use their mobile devices for many work-related applications like applications for corporate mobile, contact details of the company and its employees, and mobile dashboards. Another usage of mobile device which is very serious is downloading the business documents on their smartphones which demands regular checking's for any attack as studies show that the security of smartphones could be compromised very easily based on various threats like weakness in the authentication process, low quality of data-protection, inadequate privacy policies, operating systems like Android which is open source, malware attacks, viruses and attacks based on SMS (Li, 2016). Organizations are more prone to cyber-attacks to leak the customer-related information, which is the most critical information for any company (Tsikos, 1982). Smartphones are the most widely used device both for work and personal purposes, which invites attacks (Bud, 2018). Employees in many countries have transformed to mobile devices for their professional duties by using smartphones and tablets. Employees working in Generation-mobile (Gen-Mobile) who are early in their careers are shaping their work based on mobile devices. Based on all these usages of mobile devices, the global mobile workforce is set to jump drastically from 1.45 billion in 2016 to up to 38.8% of the global workforce and is now predicted to reach 1.87 billion by 2022 with an increase of about 42.5% of the global workforce (Raghavendra, 2013). Employees using mobile devices are more exposed to vulnerabilities which is proving to be highly disruptive to their business. This information is supported by the survey conducted by security professionals (Thavalengal, 2015) which states around 64% of the participants are uncertain whether their organization is capable of preventing mobile cyberattacks, and 94% of the participants are sure about the possibility of experiencing the attacks and 79% of the participants believe that it would be more difficult to secure their mobile devices from attacks. In another study, it has revealed that around 56% of the employees who are categorized as trusted are more prone to attacks and risk insecurity in their business (Yuan, 2012). Cybersecurity is an international issue, and it needs global efforts to tackle it. So, the World Economic Forum expressed its concern on failing to handle the global threats, especially on cybersecurity, and mentioned that the nations and also governments around the globe need to make a serious effort to handle them (Von, 2013). In another study (Määttä, 2011), it states that the cybersecurity issue could not handle if the nations work together with their own technical experts and enhance their security issues by developing tools and fix those issues efficiently. Hence an international perspective is needed to address this cybersecurity issue (Erdogmus, 2014). According to recent statistics, only less than half of the companies in the USA are in a position to handle cybersecurity (Kim, 2010). Accordingly in another study (Li, 2013) it has shown that companies in the USA reported US $21 million in one of the highest average cybersecurity costs. In UK, although they have General Data Protection Regulation (GDPR),

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

still their cases are also similar, with around 57% of the companies face cyberattacks on a regular basis (Daraghmeh, 2019). Companies in the UK also report one of the highest total average costs of cybersecurity at US$9 million (Li, 2013). The components discussed here in this section are shown below in Figure 2.

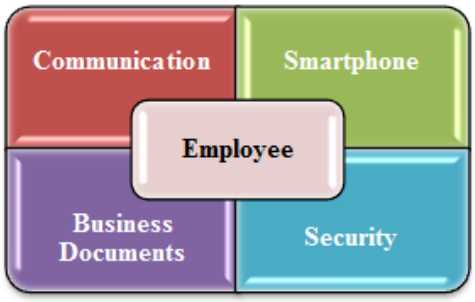

FIGURE 2
CYBERSECURITY ISSUES FOR EMPLOYEES

Security Threats on Smart Devices

Users are considered the weakest link for any kind of security issues in IT. The security in mobile devices can be handled if the users are adequately educated about the usage, and this is acting as a challenge to security aspects. The users, especially those staying at home, assume that the device is working fine as it should work, even with the default settings, without referring to the manual for complex security settings. Here the responsibility of service providers and hardware vendors also have equal share is maintaining security for the network and also managing the contents of the devices securely. The service providers can play an essential role in maintaining the safety of the device by providing add-on security services to counterpart the weakness identified in the apparatus with respect to the threats in security. Cybersecurity is not only in offices or business places. It is also taking place at homes also. The main reason for this is the mobile devices which are being used at homes. The cybersecurity issues are beyond computers as it is a continuous threat to portable devices. Since the devices which are used at homes are also very much powerful and compared to computers like mobile phones, video consoles and other devices like car navigation systems. Because of the mobility of these devices, they are more adaptable and provides extra features and functionalities, these additional functionalities and features are the source for attacks, and they attract attackers. Based on these issues, mobile devices are no more secure. The cybersecurity in UK studied by POSTnote, says the mobile devices can make an infrastructure inside the home called Critical Information Infrastructure (CII) (Cyber Security, 2011), which can store and manage the information among the devices which are used at homes. An example of this attack is the possibility of an attacker making a virus by which the secret information stored in the device could be accessed. These kinds of attacks and access to information not only affects the personal life but also could lead to serious consequences for the corporates also. Healthcare in the current times is utilizing mobile devices like mobile health. An example of this is the health device connected to the home network. This network can transmit the medical data wirelessly within the hospitals and various other related bodies. Although these kinds of devices are helping the medical staff and patients in having quick responses and providing prescriptions to the patients at the same time, these devices are not secure for critical information transmission. The manufacturers who are making these devices are not taking care with regards to the security of the data related to patient's information which sometimes is very critical. If these devices are compromised, then the essential information related to the patient would be misused, and the attackers can take control of the settings of the device, which may further lead to big disaster (Blumberg, 2011). The attackers can access the critical information stored in the device, like the name and medical information of the patients.

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

Further to accessing the patient information, the attackers could even reconfigure the parameters of the device. These all consequences are not only related to medical devices but also to the devices which are connected to the home network for other purposes. The various departments where the security threats caused by smartphones can happen are shown in Fig. 3.

The dependency on mobile devices is also reflected on an average person. According to the survey report of Juniper Networks (Juniper, 2012), 76% of the mobile users who use it on daily basis are dependent on these devices to access their complex and personal information like online banking data or personal medical data and medication details. Also, a similar situation is occurring for businessmen's who are dependent on mobile devices for their business purposes. According to another study, as much as 89% of businessmen are dependent on mobile devices for their daily transactions. These transactions are sometimes very sensitive, which is mostly related to business dealings. Similar to the medical health data attacks, these attackers also try to intervene in the business transactions and try to acquire that sensitive information. These kinds of cyber-attacks happen when people in business use mobile devices in vast networks. Another issue is the Android applications which are usually downloaded with the third-party market. These malicious applications can access the root functionality of the devices and then change it to botnet soldiers, and these changes have occurred without the user's consensus. By downloading these applications, people unwillingly download malware to their own smartphones without their knowledge and consent. This malware then attacks the mobile devices acting as a legitimate body and then starts intercepting the critical data for malicious use. These third-party applications which were mixed in the Android were successfully caught and then removed from the list of Android market as they contained malware in them. These malware contained applications were around 50 of them; these applications were a copy of the legitimate publishers, which were altered to include malware.

FIGURE 3
SECURITY THREATS IN SMART DEVICES

In another study conducted by Juniper Networks Mobile Threat Centre (MTC) (Juniper, 2012) has reported as many as 155 % of the increase in mobile malware attacks in 2011 compared to previous years in almost all the platforms. Also, with regards to Android malware, there is an increase of about 3000 % during 2011. Based on these statistics and numbers, a significant increase in malware was reported in third-party Android applications enjoying the same privileges of an actual application available in the Google Play Store. The reason for this increase in the numbers is, in the past, any Android developer had the privilege to develop an application and post them immediately at the official Android Market without screening the application for the presence of malware and inspecting the application. Another reason for the drastic increase in malware is due to the blending of Google Android dominant market and smartphones and their share, which was around 68.8% during 2012, and also the absence of

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

efficient security control methodology to control the applications which are being posted on Android application markets. In the recent study, the reports state that as many as 700,000 apps have crossed 15 billion downloads in the Google Play Store. As these numbers are increasing so also the money stealing malware are also increasing based on the security firm Fortinet which was done during 2006-2011.

Authentication

In this section, various authentication techniques will be discussed. The discussion would be based on a comparative study among different authentication methods which are based on type of identity information for authentication. Basically, identity information is used for authentication which are categorized into three classes or metrics: 1) Knowledge, 2) Biometrics, and 3) Ownerships (O'Gorman, 2003). Further, the authentication metrics are again separated into four different sections based on the mobile authentication methods. Those four categories are as follows: a) authentication based on information, b) authentication based on biometrics, c) authentication based on behavior and d) authentication based on double factor. The major components of authentication are displayed as shown in Fig. 4.

Authentication Based on Information

A knowledge-based authentication system is a traditional way of verifying the user credentials, especially for mobile devices, since it has a long history of usage among ordinary people. This method uses the knowledge which is specific and secret to that user for authentication check. It can be in text form or graphical form. The text would be some personal password that contains digit PINs and alphabetical characters, and in the graphic form, it could be pattern lock (Uellenbeck, 2013) or click, which is secret points in the picture (Chiasson, 2007). The knowledge-based authentication is straightforward where the user gives the secret information through the touch screen on the smartphone, and the device verifies the identity and clears the authentication. Since it is very simple to authenticate, it is calling problems for easy theft and leakage of knowledge. Because anyone could easy pass the authentication by retrieving the secret code. The attackers usually read the secret information by shoulder-surfing wherein the user's private information is tracked by the user's finger moments which remind on the touch screen (Aviv, 2010). Other methods also by which the attackers steal the secret knowledge-based authentication and leak the critical information. Those methods are as follows: System timing information, motion sensor (e.g., system timing information (Song, 2001), motion sensors (Miluzzo, 2012) and wireless signals (Li, 2016) on the mobile device, which could be used to infer the secret in- put by capturing the hand movement dynamics. Because of these threats, the authentication based on knowledge is now not sufficient to verify the user.

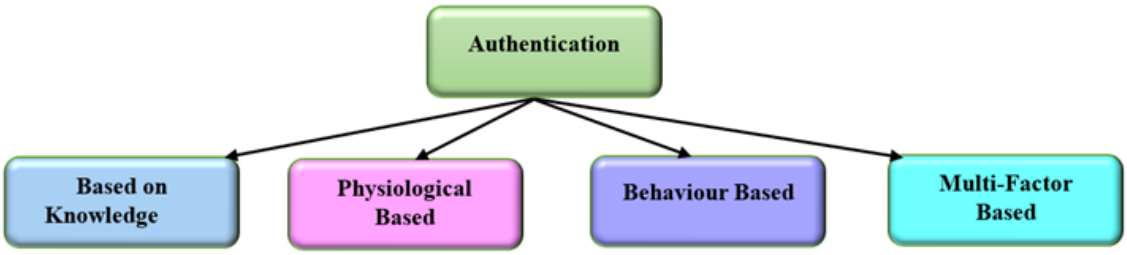

FIGURE 4
AUTHENTICATION TECHNIQUES

Authentication Based on Biometrics

Physiological Biometric-based authentication is applied to many mobile devices in addition to knowledge-based authentication. Physiological biometric authentication is better

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

than knowledge-based authentication. It is convenient to handle as it doesn't need the user to remember the authentication code like in knowledge-based. This authentication method is also more secure since it exploits the very exclusive human biometric characteristics like fingerprints, iris patterns, hand geometry, and face contour. This technique is more confident as the codes to authenticate are also very unique to the user and cannot be matched with others easily. But the difficulty faced in this approach is recording the biometric information into the system. Mobile devices need a devoted sensor to capture the characteristics of the user's body parts, like catching the fingerprints needs a special scanner (Tsikos, 1982) accompanied by a depth camera (Bud, 2018), to capture iris information, an iris reader is required in order to read from the Samsung smartphones (GallesoSamsung, 2016). Although authentication is very powerful, getting the information stored into the devices is a big challenge as it needs expensive sensors dedicated to this purpose. These expensive sensors are available only at high-end mobile devices, which are very few and are limited to access, and this is leading to stop the popularity of this authentication method to adopt in practice. According few studies (Raghavendra, 2013; Thavalengal, 2015; Yuan, 2012) it is recommended to use the commonly available cameras into mobile devices to take the physiological biometrics like fingerprints, eyes, and ear information for the user's authentication. This approach looks practical, but the reliability of these systems is a bit low when compared with the dedicated sensors. Still, these systems get affected by the attackers as discussed in this work (Zezschwitz, 2013; Määttä, 2011; Erdogmus, 2014), there it has shown that the attackers are able to crack the user's physiological biometric information like fingerprints and face recognition. But the physiological biometric is almost impossible to alter, but if this information is cracked, then they would be no other option left, and all the information could be lost, and in future this kind of authentication could become permanently insecure. Based on these issues, most of mobile device users do not adopt this kind of physiological biometric authentication.

Authentication Based on Behavior

This kind of authentication is getting a lot of attention during the current times. This technique exploits the behavior biometrics, which captures the user's unique behavioral characteristics and records it for authentication. These users' habit is used as an authentication code. An example of this authentication is, the style of tapping or swiping the user does on the touch screen and the movements of the fingers. These all activities are recorded as an authentication code which is unique with other users and stored as a pattern of behavior used for authentication (Kim, 2010; Li, 2013). Another authentication method under behavioral biometric is walking and speaking, these activities can also be used for authentication wherein it could be stored as voice patterns to utilize as an authentication key to distinguish among different users. The general users are giving priority to behavioral biometric then the physiological biometric-based authentication. The reason for their accepting behavioral biometric is its less private information is stored compared to the unchanged body traits. Another reason is the availability of low-cost sensors, which are readily available and easy to use on mobile devices. These behavioral biometrics are usually extracted by the user's daily activities in a non-intrusive manner. This technique frequently saves the activities of the users and asks for their identity proof occasionally and updates the information, and allows to enable the application for long-term protections. But, there are few drawbacks as the mobile devices which have sensors embedded in them suffer from low sampling rates and low fidelity. This causes a high false rejection rate and a fall of reliability. This the researchers are focusing on enhancing the reliability of this system by reducing the false rejection rate.

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

Authentication Based on Double Factor

As the name says, it is two-factor authentication means the users have to give two authentication codes. This authentication technique is more secure than the single factor. An example of this authentication is: the system might ask the user to provide multiple biometrics like fingerprints, voice, and face ID in order to successfully pass the authentication. Sometimes the system also asked to input both the secret code, which is based on knowledge and plus biometric information, step-by-step during the verification process. This authentication technique is very difficult to break by the intruder and might need more effort to break it successfully. At the same time, the users also face difficulty while opening the system all the time giving multiple authentication codes to verify, which usually takes more time than the single-factor authentication. The example is, the users should follow these steps: first, take the photo to clear the face ID then followed by thumb fingerprint scanning, then entering the password on the touch screen. All these steps to unlock the phone every time is time-consuming and also not comfortable in quick situations. Single-factor authentication is less robust when compared with two-factor authentication. The software token and also the hardware identifiers like MAC address are less secure when single-factor authentication is applied. But this could be enhanced by upgrading the authentication by adding a knowledge-based factor-like biometric-based factor. This addition of factors had ultimately enhanced the security level and is called two-factor authentication. Although two-factor authentication is more secure and robust compared to single-factor it still lacks strength in security. Like for example, the intruder can forge the software and hardware token and prove the ownership and also at the same time can give the knowledge-based secret biometric information which was stolen as input for authentication. So, to counter this issue, a new and improved security code should be implemented, which should be more robust than a two-factor authentication system.

Machine Learning

Technologies related to smart cities are combined with Android OS applications as these applications are supporting the smart city requirements. Android is playing an essential role in various fields in the current development phase of the earth. These applications are helping different sectors like competent government, intelligent transportation, and other energy resources management (Daraghmeh, 2019; Turjman, 2019). The facilities provided by Android is allowing developers to utilize them in their applications. Still, at the same time, it is acting as a source to attackers like malware which is targeting the Android to cause serious threats which are leading to financial loss, leakage of critical data, and security concerns for nations (Yaokumah, 2020). Based on the excellent features offered by Android and flexible to adopt technologies, it has captured as much as 80% of smartphone users. But, at the same time, it has become a significant source for malware attacks (Nassiri, 2020). Based on this report (Deebak, 2019), as many as four million fresh malicious applications were developed during 2019. The average time in which the hackers create an infected APP is around every eight seconds. This statistic of malware attacks and the development of malicious applications are alarming and becoming a source of a major threat to cyber-security. So, well-managed and efficient detection methods are need of the hour for Android malware, and it needs urgent attention from computer professionals to develop tools to detect these attacks especially to improve mobile security (Lv, 2019).

Malware detection methods are classified into two categories based on the process by which they are detected like signature-based method or behavior-based method. In the current scenario, signature-based malware detection is working fine for the previously detected malware which was done with the help of anti-malware vendors. But the polymorphic malware is not yet detected, which can change the signatures. Also, new malware which is expected to occur in the future cannot be detected by these traditional methodologies. So, the best solution that is

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

recommended by researchers is utilizing the heuristic analysis along with the machine learning techniques that could provide better solutions with higher efficiency for detection. As practice has shown, the traditional approach to the field of malware detection, which is based on signature analysis (Mart, 2019), is not acceptable for detecting unknown computer viruses. In the current times, mobile security researchers are working hard to counter the risk of malicious Apps. They are proposing various defense approaches especially novel methodologies to detect malware. These methodologies are based on machine learning techniques which are proving to be very efficient in various research fields in solving their problems. Further to machine learning, they are also implementing advanced techniques like deep learning, which is attracting security researchers of various fields to implement this technique (Xu, 2018; Amin, 2020). The process of utilizing machine learning techniques for the detection of state-of-the-art malware attacks could be generally classified into three categories: Static feature (Wang, 2014; Faruki, 2013), dynamic feature (Wong, 2016; Cai, 2018), and mixed feature (Chen, 2016; Lindorfer, 2015). The most critical aspect of machine learning to get got accuracy in the result is feature selection. It is also used during training the model. The more accurate the features are, the more robust the model is, and more would be the classification accuracy (Vinod, 2019; Ucci, 2019; Feng, 2018). The feature selection is a crucial step in machine learning to enhance the performance of the model and also to make a robust model all the irrelevant features and redundant features should be removed, and refined features which play a significant role should be selected. This process is time-consuming as the result of machine learning depends on this step. In this section malware detection techniques are discussed. These are three techniques which are based on machine learning for Android malware detection. After this section an advanced state-of-the-art technique would be discussed, which are based on deep learning methodology.

ML-based Android Malware Detection Methods

There are two types of analysis being utilized in machine learning techniques, one is the static analysis, and the other is dynamic Analysis

Static Analysis

The authors in this work (Fereidooni, 2016) have applied various classical machine learning classifiers also deep neural networks and proposed a system to detect malware attacks on Android system. The major contribution was extracting the relevant features, which are also sensitive. They have designed and developed a static analysis tool for the feature extraction step. The outcome of this approach is around 97.3% of accuracy for the true positive rate. In another work (Aafer, 2013) f or malware detection, the authors here have applied different approach wherein the sensitive packages which cause the malware attacks are detected. These are called package-level API calls, which are found in common inside malicious apps. This approach is also capable of extracting another package level which gives the feature details for a large set of Android malware. This technique gave good results with around 99% of the accuracy and false positive rate as 2.2%. In another work (Arp, 2014), the significant contribution was working on extracting features. The features were extracted from the manifest file and from the source code of the application. These features were then trained with an SVM classifier. The classifier was able to classify and detect malware based on the features provided and further, it achieved good accuracy and performance for the detection of malware. The authors in this work applied a different approach to detect the malware (Zhang, 2014), semantic features were extracted from the weighted contextual API. These APIs were used to draw dependency graphs further to classify them as Android malware or not. The proposed system is capable of effectively fighting against malware. Another feature extraction technique was proposed by (Mariconti, 2016), to detect malware. Here the authors have applied the Markov chain to the sequence of API calls and then extract the relevant features. After removing these features, then traditional

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

classification methodology is used to classify and detect the malware. In this work (Wu, 2012), features were extracted from permissions and API calls. These features were extracted from the files stored in the Android manifest file. These extracted features were then applied for classification using the K-nearest neighbor algorithm. These classifiers are used to classify benign and malware apps. The results were further improved after applying the K-means algorithm

Dynamic Analysis

In this work (Yan, 2012), a dynamic android malware analysis technique is proposed for the detection of possible malware. Here the authors have constructed OS-level and Java-level semantic views. The system is capable of tracking the changes in the files such as threads and processes. It can detect the malware through system calls and Dalvik instructions. These details are provided for the dynamic analysis.

RECOMMENDATIONS

In this section, some of the essential recommendations are listed, which are available in the literature for the justification of malware or malicious attacks. These recommendations would help and facilitate the efficient utilization of smartphones. Also, these recommendations would benefit in improving the security concerns for smartphones in the coming future. Fig. 5 lists those parties that can benefit from these recommendations.

Recommendations to Smartphone Users

Educating the users about security threats and the best practice to counter those attacks is the essential step, and it is highly recommended to update them about the latest attacks (Hadadi, 2013). The main reason for this recommendation is, the users are the first line of defense and need to be educated to counter those attacks. Only educating them is not enough to save them from attacks. Instead, they need to ab aware of how to protect themselves and should be able to detect the future for malware threats (Pieterse, 2013; Adebayo, 2014). Other recommendations for the users are: they should update themselves for the changes which have been done on their smartphones by the corporates who constantly develop latest technologies to protect their system from attacks. The users should constantly educate themselves for the latest changes adopted for the safety policies (Bernik, 2012).

Technical Guidelines for the Smartphone Users

Mobile users must protect their devices from any kind of mobile malware. They should take precautionary steps to save their smartphones. They should avoid being victims to cybercrimes (Pieterse, 2013). They can do so by properly installing the latest anti-virus and apps related to security. The users must also be actively checking their roots of connections and disconnect their Bluetooth if not in use to avoid unnecessary connecting to malicious devices. The users must also have a check on their location setting and need to switch it off when not needed to avoid getting track of their physical presence. The users must also use the pattern lock facility available on the smartphones to block their settings and block unauthorized access to the devices. Also, it is recommended to the users to constantly update their passwords and avoid usage of passcode that could be effortlessly predicted by illegal people. The users must also get an awareness about the sensitive data stored in the device and also be aware of the possible threats and risks on saving such information on smartphones.

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

Usage Restrictions from the Users of Smartphone

Another recommendation to mobile users is not to give their devices to strangers and leave their devices unattended. This might invite problems and possible attacks on the security of the device (Adebayo, 2014). The users are recommended to regularly check the current number of accounts that are signed in on their smartphones. The users must also check the permission settings of the apps which are being installed on their devices. As said above, the users must have a check on their device setting and frequently check them if they get changed by attackers or disabled by the malware; they should be able to detect the changes if they occur on the settings. Users are also recommended to have an eye on small mobile features like the battery life and data consumption details to know any change in them because of the malware. Also, it is recommended to check the Bluetooth and Wi-Fi settings regularly and also the devices connected through this source.

Users Monitoring the Apps Installed

The users need to work on the OS of the smartphones they use. The OS needs to be updated regularly, which helps the device get safe and protected from malware. Once the OS is updated, the users must also update the anti-virus and security apps also. The users should check the apps which are not used frequently on their smartphones and delete them as some malware penetrates through these apps (Mikhaylov, 2013; Wei, 2012). The users should be aware of whom to contact and how to contact if they feel any attack or breach of security. The users who are installing any new app should be careful about requesting private information about the user by writing or sending through SMS. The users should be cautious while downloading and installing apps from unknown sources (Liang, 2014).

FIGURE 5
RECOMMENDATIONS FOR MOBILE USERS, RESEARCHERS AND GOVERNMENT AUTHORITIES

Recommendations to Researchers

Researchers should be encouraged from different fields to form a community and take this research study with the aim to develop robust open source apps which can play an important role in reimbursing the security threats and vulnerability from various apps which sometimes come from the official smartphone market also (Batten, 2016). There are many studies conducted for the development of viruses, and further products were introduced in the market, but very few researches are done on smartphone security, and it is currently in the infancy stage. So, it is highly recommended for researchers to take up this research field to explore more security threats related to the smartphone. Since the rapid increase in smartphone usage, the malware is also increasing accordingly, and the development of software related to anti-virus is also imperative. As introduced by (Zhou, 2012), it is considered as the best security app which was able to detect as much as 79.6% of malware. So, this encourages to take further initiatives to develop next-generation of anti-mobile malware (Xin, 2017). One of the most robust security

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

monitoring systems available in the literature is the honeypot-monitoring system for mobile communication. But, it has some shortcomings, such as communication range support which is limited. Another direction for researchers to take up this topic is the performance of anti-virus apps. However, various anti-virus app is developed which can counter the attacks. Some of the attacks are made through Wi-Fi which needs to be studied. The researchers are expected to analyze the architecture of the network switch to avoid invasion of malware (Song, 2012). Another research direction is to explore new defense mechanisms which can be capable of managing the malware (Su, 2012). Researchers can work on security apps at different levels. They can work on a single app which is having no relationship with other apps similarly comparing the app with similar attributes and further working on app with comparing it with related apps, and further research by comparing the developed app with similar category with the assumption that they all have similar attributes (Kuehnhausen, 2013). The researchers are encouraged to adopted machine learning techniques to effectively detect the malware and come up with excellent results for large-scale experiments since none of the currently available techniques are fully accurate in detecting malicious behavior. As the current technique is a single analysis based and is insufficient (Guido, 2013). So, a new and enhanced analysis methodology is needed, which can be integrated and further plugged into the current techniques for enhanced accuracy (Eder, 2013). Researchers are recommended to work on botnet malware detection as it is not taken seriously in recent time. Many research works are conducted on security issues for detecting the malware, but botnet malware is considered as more serious. This is suggested based on the recent survey, which says out of 1260 samples of mobile malware, 93% of them belong to botnet malware which motivates the researchers to take up this topic (Abdullah, 2014).

Recommendations to Government Authorities

The government can play an essential role in promoting the awareness of security issues related to smartphones. This awareness can be achieved by carefully handling the problem and carried out efficiently. The following are the essential recommendations for government authorities to carry on security-related concerns. The establishment of homeland security should be equal to sharing of information. This rule should be customized according to the current needs and requirements. The governments should establish collaborations among other countries such as Europe, US, South Korea, and France to make a standard protocol and an agreement with Apple and Android devices to follow a standard rule and avoid unauthorized standards for examination. Also, it is recommended to government authorities to establish laboratories dedicated for cybercrimes and forensics studies and invest more in this field of research. The government authorities can establish certain rules and standards for acquiring data for mobile phones. Government authorities must ensure the proper availability of tools that can perform the examination on smartphones for the detection of forensics and other vulnerabilities. If smartphones are imported into the country, the government authorities should ensure the issuance of security checks by installing anti-virus and other apps to avoid attacks through the smartphones. They should form a collaboration with these app developing companies. The government can also form and implement policies that would require QR code that can enforce certain rules, like expiration dates for distributers to check if they delivered the smartphones before these expiration dates. Government can invest by providing training programmes and campaigns for the awareness of security issues on smartphones for their users (Karim, 2015).

CONCLUSION

In this work, cybersecurity concepts are discussed, which are revolving around security and authentication details. Initially, cybersecurity is discussed in general about the statistics and the problems faced by general users of the internet, then further to the study, company employee

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

was discussed and their issues related to cyber-attacks. Then, security aspects related to smartphones are discussed, focusing on the issues related to users, medical data security, banking data security, and company employees who are facing issues with the usage of smartphones. Further to the study, authentication is discussed because this is the main contribution to this field of research. Authentication is very important as this is the key to avoid any kind of attack. If the authentication steps are robust, then any kind of attack can be tackled. So, basically, four kinds of authentications are discussed for the readers to explore further. There are so many techniques available to develop robust authentication techniques. In this, machine learning is playing an important role. So, machine learning concepts related to cybersecurity are discussed. After all these technical contents, few recommendations are drafted for users, researchers, and government authorities.

ACKNOWLEDGMENT

This research was funded by the Deanship of Scientific Research at Princess Nourah Bint Abdulrahman University through the Fast-track Research Funding Program.

CONFLICTS OF INTEREST

The author declare that they have no conflicts of interest to report regarding the present study.

REFERENCES

Cyber Security in the UK,' Houses of Parliament September (2011).

Blumberg, J. (2011). 'Cybersecurity, health care, and mobile devices,' in dartmouth now.

Juniper, 'Trusted Mobility Index,' (2012).

Juniper, 'Juniper Networks 2011 Mobile Threats Report,' Juniper Networks Mobile Threat Center (MTC), 2012."

L. O'Gorman. (2003). "Comparing passwords, tokens, and biometrics for user authentication," *Proc. IEEE*, *91*(12), 2021–2040.

Uellenbeck, S., Dürmuth, M., Wolf, C. & Holz, T. (2013). "Quantifying the security of graphical passwords: The case of android unlock patterns," in *Proceedings of the 2013 ACM SIGSAC conference on Computer \& communications security*, 161–172.

Chiasson, S., Van Oorschot, P.C., & Biddle, R. (2007). "Graphical password authentication using cued click points," in *European Symposium on Research in Computer Security*, 359–374.

Aviv, A.J., Gibson, K.L., Mossop, E., Blaze, M., & Smith, J.M. (2010). Smudge attacks on smartphone touch screens. *Woot*, *10*, 1–7.

Song, D.X., Wagner, D.A., & Tian, X. (2001). Timing analysis of keystrokes and timing attacks on ssh. in *USENIX Security Symposium*.

Miluzzo, E., Varshavsky, A., Balakrishnan, S., & Choudhury, R.R. (2012). "Tapprints: Your finger taps have fingerprints," in *Proceedings of the 10th international conference on Mobile systems, applications, and services*, 323–336.

Li, M. (2016). "When CSI meets public WiFi: Inferring your mobile phone password via WiFi signals," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 1068–1079.

Tsikos, C. (1982). Inventor, siemens corp, assignee. capacitive fingerprint sensor. United States patent US *4*,353,056 5.

Bud, A. (2018). Facing the future: The impact of Apple FaceID. *Biometric Technol. Today*, *1*, 5–7.

GallesoSamsung, M. (2016). Galaxy Note 7: An easy guide to the best features, first rank publishing.

Raghavendra, R., Busch, C., & Yang, B. (2013). Scaling-robust fingerprint verification with smartphone camera in real-life scenarios. in *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 1–8.

Thavalengal, S., Bigioi, P., & Corcoran, P. (2015). Iris authentication in handheld devices-considerations for constraint-free acquisition," *IEEE Trans. Consum. Electron.*, *61*(2), 245–253.

Yuan, L., & Chun Mu, Z. (2012). "Ear recognition based on local information fusion," *Pattern Recognit. Lett*, *33*(2), 182–190.

Von Zezschwitz, E., Koslow, A., De Luca, A., & Hussmann, H. (2013). "Making graphic-based authentication secure against smudge attacks," in *Proceedings of the 2013 international conference on Intelligent user interfaces*, 277–286.

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

Määttä, J., Hadid, A., & Pietikäinen, M. (2011). Face spoofing detection from single images using micro-texture analysis," in *2011 international joint conference on Biometrics (IJCB)*, 1–7.

Erdogmus, N., & Marcel, S. (2014). Spoofing face recognition with 3D masks," *IEEE Trans. Inf. forensics Secur.*, *9*(7), 1084–1097.

Kim, D. (2010). Multi-touch authentication on tabletops," in *Proceedings of the SIGCHI conference on Human factors in computing systems*,1093–1102.

Li, L., Zhao, X., & Xue, G. (2013). Unobservable re-authentication for smartphones.," in *NDSS*, *56*, 57–59.

Daraghmeh, M., Al Ridhawi, I., Aloqaily, M., Jararweh, Y., & Agarwal, A. (2019). "A power management approach to reduce energy consumption for edge computing servers," in *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*, 259–264.

Al-Turjman, F., Zahmatkesh, H., & Mostarda, L. (2019). Quantifying uncertainty in internet of medical things and big-data services using intelligence and deep learning. *IEEE Access*, *7*, 115749–115759.

Yaokumah, W., Rajarajan, M., Abdulai, J.D., Wiafe, I., & Katsriku, F.A. (2020). *Modern Theories and Practices for Cyber Ethics and Security Compliance*. IGI Global.

Nassiri, M., HaddadPajouh, H., Dehghantanha, A., Karimipour, H., Parizi, R.M., & Srivastava, G. (2020). Malware elimination impact on dynamic analysis: An experimental machine learning approach," in *Handbook of Big Data Privacy*, Springer, 359–370.

Deebak, B.D., Al-Turjman, F., Aloqaily, M., & Alfandi, O. (2019). An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT," *IEEE Access*, *7*, 135632–135649.

Lv, Z., Mazurczyk, W., Wendzel, S., & Song, H. (2019). Guest Editorial: Recent Advances in Cyber-Physical Security in Industrial Environments. *IEEE Trans. Ind. Informatics*, *15*(12), 6468–6471.

Martin, I., Hernández, J.A., & de los Santos, S. (2019). Machine-Learning based analysis and classification of Android malware signatures. *Futur. Gener. Comput. Syst.*, *97*, 295–305.

Xu, K., Li, Y., Deng, R.H., & Chen, K. (2018). Deeprefiner: Multi-layer android malware detection system applying deep neural networks. in *2018 IEEE European Symposium on Security and Privacy (EuroS\&P)*, 473–487.

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. *Futur. Gener. Comput. Syst*, *102*, 112–126.

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 Trans. Inf. Forensics Secur*, *9*(11), 1869–1882.

Faruki, P., Ganmoor, V., Laxmi, V., Gaur, M.S., & Bharmal, A. (2013). AndroSimilar: robust statistical feature signature for Android malware detection," in *Proceedings of the 6th International Conference on Security of Information and Networks*, 152–159.

Wong, M.Y., & Lie, D. (2016). IntelliDroid: A Targeted Input Generator for the Dynamic Analysis of Android Malware. in *NDSS*, *16*, 21–24.

Cai, H., Meng, N., Ryder, B., & Yao, D. (2018). Droidcat: Effective android malware detection and categorization via app-level profiling. *IEEE Trans. Inf. Forensics Secur*, *14*(6), 1455–1470.

Chen, S., Xue, M., Tang, Z., Xu, L., & Zhu, H., (2016). Stormdroid: A streaminglized machine learning-based system for detecting android malware. in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 377–388.

Lindorfer, M., Neugschwandtner, M., & Platzer, C. (2015). Marvin: Efficient and comprehensive mobile app classification through static and dynamic analysis. in *2015 IEEE 39th annual computer software and applications conference*, *2*, 422–433.

Vinod, P., Zemmari, A., & Conti, M. (2019). A machine learning based approach to detect malicious android apps using discriminant system calls. *Futur. Gener. Comput. Syst*, *94*, 333–350.

Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. *Comput. & Secur.*, *81*, 123–147.

Feng, P., Ma, J., Sun, C., Xu, X., & Ma, Y. (2018). A novel dynamic Android malware detection system with ensemble learning. *IEEE Access*, *6*, 30996–31011.

Fereidooni, H., Conti, M., Yao, D.,& Sperduti, A. (2016). ANASTASIA: ANdroid mAlware detection using STatic analySIs of Applications. In *2016 8th IFIP international conference on new technologies, mobility and security (NTMS)*, 1–5.

Aafer, Y., Du, W., & Yin, H. (2013). Droidapiminer: Mining api-level features for robust malware detection in android. In *International conference on security and privacy in communication systems*, 86–103.

Arp, D., Spreitzenbarth, M., Hubner, M., Gascon, H., Rieck, K., & Siemens, C. (2014). "Drebin: Effective and explainable detection of android malware in your pocket.," in *Ndss*,*14*, 23–26.

Zhang, M., Duan, Y., Yin, H., & Zhao, Z. (2014). Semantics-aware android malware classification using weighted contextual api dependency graphs. in *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, 1105–1116.

Mariconti, E., Onwuzurike, L., Andriotis, P., De Cristofaro, E., Ross, G., & Stringhini, G. (2016). Mamadroid: Detecting android malware by building markov chains of behavioral models," *arXiv Prepr. arXiv1612.04433*.

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.

Wu, D.J. (2012). Droidmat: Android malware detection through manifest and api calls tracing," in *2012 Seventh Asia Joint Conference on Information Security*, 62–69.

Yan, L.K., & Yin, H. (2012). Droidscope: Seamlessly reconstructing the and dalvik semantic views for dynamic android malware analysis," in *21st Security Symposium Security*, *12*, 569–584.

Al-Hadadi, M., & Al Shidhani, A. (2013). Smartphone security awareness: Time to act," in *2013 international conference on current trends in information technology (CTIT)*, 166–171.

Pieterse, H., & Olivier, M.S. (2013). Security steps for smartphone users," in *2013 Information Security for South Africa*, 1–6.

Adebayo, O.S., & Aziz, N.A. (2014). Techniques for analysing Android malware," in *The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M)*, 1–6.

Bernik, I., & Markelj, B. (2012). "Blended threats to mobile devices on the rise," in *International Conference on Information Society (i-Society 2012)*, 59–64.

Mikhaylov, D., Zhukov, I., Starikovskiy, A., Kharkov, S., Tolstaya, A., & Zuykov, A. (2013). Review of malicious mobile applications, phone bugs and other cyber threats to mobile devices," in *2013 5th IEEE International Conference on Broadband Network \& Multimedia Technology*, 302–305.

Wei, T.E., Jeng, A.B., Lee, H.M., Chen, C.H., & Tien, C.W. (2012). Android privacy," in *2012 international conference on machine learning and cybernetics*, *5*, 1830–1837.

Liang, S., Du, X., Tan, C.C., & Yu, W. (2014). An effective online scheme for detecting Android malware," in *2014 23rd international conference on computer communication and networks (ICCCN)*, 1–8.

Batten, L.M., Moonsamy, V., & Alazab, M. (2016). "Smartphone applications, malware and data theft," in *Computational intelligence, cyber security and computational models*, Springer,15–24.

Zhou, Y., & Jiang, X. (2012). Dissecting android malware: Characterization and evolution," in *2012 IEEE symposium on security and privacy*, 95–109.

Xin, K., Li, G., Qin, Z., & Zhang, Q. (2012). "Malware detection in smartphone using hidden Markov model," in *2012 fourth international conference on multimedia information networking and security*, 857–860.

Song, Y., Zhu, X., Hong, Y., Zhang, H., & Tan, H. (2012). A mobile communication honeypot observing system," in *2012 fourth international conference on multimedia information networking and security*, 861–865.

Su, X., Chuah, M., & Tan, G. (2012). Smartphone dual defense protection framework: Detecting malicious applications in android markets. In *2012 8th International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, 153–160.

Kuehnhausen, M., & Frost, V.S. (2013). Trusting smartphone apps? To install or not to install, that is the question," in *2013 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, 30–37.

Guido, M., Ondricek, J., Grover, J., Wilburn, D., Nguyen, T., & Hunt, A. (2013). "Automated identification of installed malicious Android applications," *Digit. Investig*, *10*, S96--S104.

Eder, T., Rodler, M., Vymazal, D., & Zeilinger, M. (2013). "Ananas-a framework for analyzing android applications," in *2013 international conference on availability, reliability and security*, 711–719.

Abdullah, Z., Saudi, M.M., & Anuar, N.B. (2014). "Mobile botnet detection: Proof of concept," in *2014 IEEE 5th control and system graduate research colloquium*, 257–262.

Karim, A., Shah, S.A.A., Bin Salleh, R., Arif, M., & Noor, R.M. (2015). "Mobile botnet attacks--an emerging threat: classification, review and open issues," *KSII Trans. Internet Inf. Syst.*, *9*(4), 1471–1492.

Citation Information: Aldakheel, E.A., & Zakariah, M. (2021). Mobile devices and cybersecurity issues authentication techniques with machine learning. *Journal of Management Information and Decision Sciences, 24*(S6), 1-15.