COMPUTERS & SECURITY 73 (2018) 519–544

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Mobile phishing attacks and defence mechanisms: State of art and open research challenges

Diksha Goel, Ankit Kumar Jain *

Computer Engineering Department, National Institute of Technology, Kurukshetra, India

ARTICLE INFO

Article history:
Received 10 October 2017
Received in revised form 5 December 2017
Accepted 13 December 2017
Available online 20 December 2017

Keywords:
Mobile phishing
Smartphones
Cyber security
Social engineering
Mobile malware
Machine learning

ABSTRACT

Phishing is an online identity theft in which an attacker tries to steal user's personal information, resulting in financial loss of individuals as well as organisations. Nowadays, mobile devices especially smartphones are increasingly being used by the users due to a wide range of functionalities they provide. These devices are very compact and provide functionalities similar to those of desktop computers due to which attackers are now targeting the mobile device users. However, detection of mobile phishing attack is a different problem from desktop phishing due to the dissimilar architectures of both. Moreover, identification of mobile phishing attack with high accuracy is an important research issue as not much amount of work has been done in this field. Many anti-phishing solutions for mobile devices have been proposed till date but still there is a lack of a full fledge solution. The primary objective of this paper is to do a detailed analysis on mobile phishing – attacking techniques and defence mechanisms. We present this paper in four folds. First, we discuss in detail about mobile phishing attack, its history, motivation of attackers, and security concerns of smartphones. Second, we analyse various mobile phishing attacks and provide a taxonomy of the same. Third, we provide taxonomy of numerous recently proposed solutions that detect and defend users from mobile phishing attacks. Fourth, we discuss different issues and challenges faced by researchers while dealing with mobile phishing attacks. In addition, we have also discussed datasets and evaluation matrices used by researchers for evaluating their approaches.

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

Cyber threats such as unsolicited emails, malicious software, viruses, spyware, Distributed Denial of Service (DDoS) attacks, and social engineering attacks exploit the security of smartphone devices. One such cyber threat is "Phishing Attack". Phishing is an online spoofing mechanism in which social engineering messages are communicated via electronic communication channels to prompt users to perform certain actions for the benefit of attacker (Khonji et al., 2013). Attackers launch phishing attack for social or financial gains. Although, a significant amount of work has been done to detect phishing attacks but still it is one of the most serious crimes over the Internet. A recent report by Anti-Phishing Working Group (APWG) shows that in 2016, the total number of unique phishing attacks detected were 1,220,523, which is an increase of 65% over 2015 (Anti-Phishing Working Group [APWG], 2016a, 2016b, 2016c, 2016d).

Use of smartphones has become prevalent due to their small size, long battery life, and portability (Foozy et al., 2013). Easy availability of smartphones and low-cost data plans have led

* *Corresponding author.*
E-mail address: ankit.jain2407@gmail.com (A.K. Jain).
https://doi.org/10.1016/j.cose.2017.12.006
0167-4048/© 2017 Elsevier Ltd. All rights reserved.

to an exponential increase in the usage of smartphones. Not only young or techno-freak people are using smartphones, but it is used by people of all age groups. With an increase in use of smartphones, security threats related to these devices have also increased. These devices have become an attractive target for the attackers. Attackers send SMSes containing links to phishing webpages or phishing applications which when accessed, ask for the personal information from the user (CAPEC, 2017). As compared to desktop users, mobile device users are at least three times more vulnerable to phishing attacks (Kessem, 2012) and the reason for this vulnerability is small screen size, lack of identity indicators, inconvenience of user input, switching between applications, habits and preferences of mobile device users.

By exploiting the hardware limitations of these devices and careless behaviour of the users, an attacker can easily carry out phishing attack on mobile phones. There is a lack of knowledge among the users about phishing attacks and how it can be avoided (Tewari et al., 2016). According to a study, 44% of the users are not aware of the security solutions available for mobile devices (Symantec, 2017a, 2017b). Security of mobile devices is influenced by many factors, such as security threats and security requirements. We do not have any method to check if the credentials are sent to a legitimate server or any other rogue server. If Operating System (OS) of mobile devices is compromised, malicious applications can access device's camera, SMSes, contacts, and can also gain location information which in turn compromise the privacy of the users (Choudhary and Jain, 2017a). Economy is negatively affected by the phishing attacks due to financial losses that are faced by the businesses as well as the individuals (Gupta et al., 2017).

A lot of solutions have been proposed for the detection and prevention of phishing attacks, still the threat is not alleviated. Blacklisting, Uniform Resource Locator (URL) based detection, static detection, and heuristics techniques are various methods used for detecting phishing attacks. Some users make use of anti-phishing software that are available in the market. Most of these software use blacklists to detect malicious and phishing applications installed on the device but blacklist can not detect zero-day phishing attacks (Chorghe and Shekokar, 2016b). Large number of phishing websites revives and expires every day. According to APWG, on an average, a phishing site stays on the web for 4.5 days and sometimes for just few hours (Cranor et al., 2007).

The objective of this paper is to give an overview of mobile phishing attacks by considering various attacking techniques used by the attackers and solutions proposed by the researchers. Performance matrices and datasets used for experimental purpose have also been discussed. In addition, we present some of the open challenges and issues related to mobile phishing attacks.

The rest of the paper is structured as follow. In Section 2, we discuss the history, motivation, importance, and life cycle of mobile phishing attacks. Section 3 contains the performance evaluation matrices and various datasets used for experimental purposes. Section 4 describes various security concerns related to the smartphones. Section 5 presents the taxonomy of various mobile phishing attacks. In Section 6, taxonomy of some defence mechanisms is discussed. Open issues and challenges are discussed in Section 7. Finally, Section 8 concludes the paper.

2. Background

In this section, we discuss the history and evolution of the phishing attacks, motivation of the attackers, some related statistics, and life cycle of mobile phishing attacks.

2.1. History

The term "Phishing" was coined in the year 1996, when a large number of fraudulent users with fake credit card details registered on America Online (AOL) website (PHISHING.org, 2017). AOL approved these accounts without verification and attackers started using AOL system's resources. At the time of payment for the services, AOL found that most of these credit cards were invalid and accounts were fake. As a consequence, the accounts were ceased. After this, AOL started properly authenticating the credit cards. This made attackers to find other ways for obtaining AOL accounts. After that, instead of using fake accounts, attackers started stealing passwords of registered AOL users by contacting them through emails or messages that appeared to be from AOL employees and used various services on behalf of the legitimate users by using their credentials (Jain and Gupta, 2017a). Evolution of phishing attack is presented in Table 1.

2.2. Motivation

Attackers take advantage of weaknesses found in the system that are caused by the user of the system. In cyber security, humans are the most delicate link. We can technically secure our devices by using various software or plug-ins, but what if user himself reveals the password (Khonji et al., 2013). Exploiting human beings is easy as compared to exploiting systems. Lack of awareness among the users is one of the main reasons behind the success of phishing attacks. From an

Table 1 – Evolution of phishing attack.

Year	Event
1996	"Phishing" term was used for the first time
1997	Media warned users about Phishing attacks
2000	Use of key loggers for obtaining credentials
2001	Use of spam messages for phishing attacks
2003	Attackers started registering for domains that mimic like legitimate sites
2004	"Cabir", the first mobile malware was released
2005	Use of Spear Phishing attacks
2006	Use of "Man in the Middle" attack for Phishing attack; Use of VoIP to conduct phishing attacks, also known as Vishing
2008	Mobile Application Store was launched
2009	"Chat in the Middle" Phishing attack was discovered
2010	Term "Tabnabbing" was coined
2011	Gaming users hit by "Xbox Live" phishing attack
2014	110 million credit cards were compromised due to phishing scams
2015	100,000 people received phishing emails in UK
2016	500% increase in social media phishing attacks
2017	W-2 Phishing attacks affected more than 120,000 people

attacker's point of view, the motives for performing phishing attacks are as below:

- Financial benefits: Phisher steals user's login information of various online services with the help of spoofed emails that appear to originate from reputed company by sending warning messages to update information in the provided link so that they can use these credentials for financial benefits.
- Stealing personal information: Attackers may steal personal information like name, address, phone number, or email address. This information is required by the marketing companies who pay high amount for such information.
- Selling stolen identities: Sometimes instead of using the stolen identities themselves, attackers may sell these to others who might want to use these to hide their identity.
- Defame: Rivals may launch phishing attacks on a company in order to damage the market reputation of that company.
- Ransom: Attackers may perform phishing attack in order to obtain ransom by attacking the organisation or individuals who can pay ransom. Ransomware is a computer virus which when downloaded prevents access to data or threatens to publish data unless a ransom is paid.
- Propagation of attack: Attackers use phishing attacks for internal jump points within an organisation or for hiding their location.
- Exploit Security gaps: To find vulnerability and errors in someone's system so as to carry out phishing attacks in future.
- Fame and Notoriety: Sometimes new phisher or attackers carry out phishing attacks to gain popularity and recognition for their activities among peer groups.

2.3. *Statistics*

Capabilities of personal computers are combined with the pocket sized mobile phones resulting into a device called Smartphone. Smartphones give users a wide range of functionalities, such as calling, SMS, emails, downloading, gaming, audio and video playback. These rich functionalities have attracted a large number of users (Carroll and Heiser, 2010). Smartphone users are increasing every year. Currently there are 2.32 billion smartphone users worldwide which is expected to be 2.87 billion in 2020 (Statista, 2017a) as shown in Fig. 1. Mobile traffic ex-

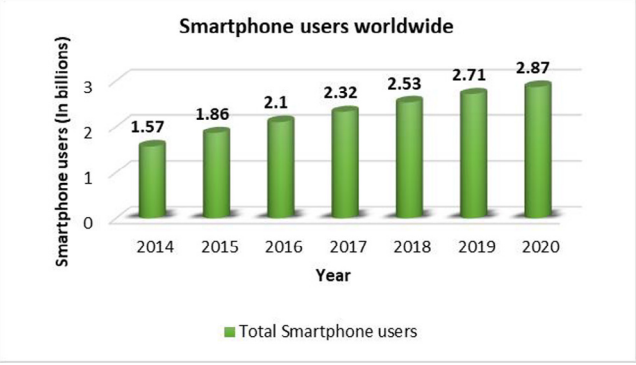

Fig. 1 – Number of smartphone users around the world.

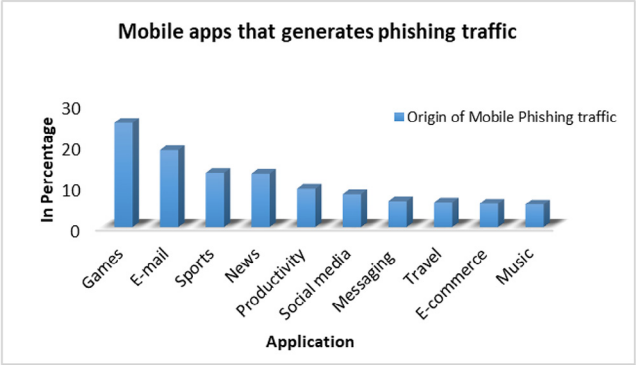

Fig. 2 – Mobile applications that generates phishing traffic.

ceeded desktop traffic for the first time in November 2016, showing a market swing about how people are currently accessing the web. Attackers are very much aware about this shift and hence targeting the mobile device users instead of desktop users.

Attackers are using various means like SMSes, emails, webpages, and mobile applications to attack mobile device users. Smishing is becoming a popular social engineering tool for the attackers. 33% of all the mobile device users have received a smishing message (Phishingpro, 2017). Phishing SMS consists of a text message and a link that redirects user to a phishing webpage. 42% of the users open this malicious link (Proofpoint, 2017). Usually, attacker tries to trick users by prompting them to click the malicious links or by installing a malicious application. Of all the security attacks on mobile devices, 12% of these attacks include a phishing URL (Wandera, 2017). Fig. 2 shows the common mobile applications that generate the phishing traffic. Gaming applications generate most of the phishing traffic in mobile phones followed by email, sports and other applications (Wandera, 2017).

In 2016, 85% of organisations have experienced phishing attacks (Wandera, 2017) and 55% of organisations have observed an increase in whaling attacks (Phishingpro, 2017). Approximately 93% of phishing attacks include ransomware. According to SANS report, phishing and ransomware are causing harm to the financial sector by aiming at organisations which can pay ransoms (SANS). Out of those organizations who calculated their losses, 32% stated that the losses were between $100,001 and $500,000. Fig. 3 shows various threats and their impact on organisations. Around 80% of organisation reported that they have faced phishing attacks and 27% of them reported that threats have significant impacts. 58% of organisations have faced spear phishing attacks or whaling attacks and 13% said that threats have a significant impact. 53% of the organisations have seen Trojan horse threat but the impact was low, i.e. 7% (SANS).

According to Cloudmark threat report, one out of every four unsolicited messages attempts to steal user's sensitive information (Security through education, 2017). 28% of mobile device users receive unsolicited messages everyday while 58% of users receive at least one unsolicited message in a week (Mobile Ecosystem Forum, 2017). Most of the users on receiving these unwanted messages either ignore them or do not take any actions. Studies have shown that 54% of the users delete

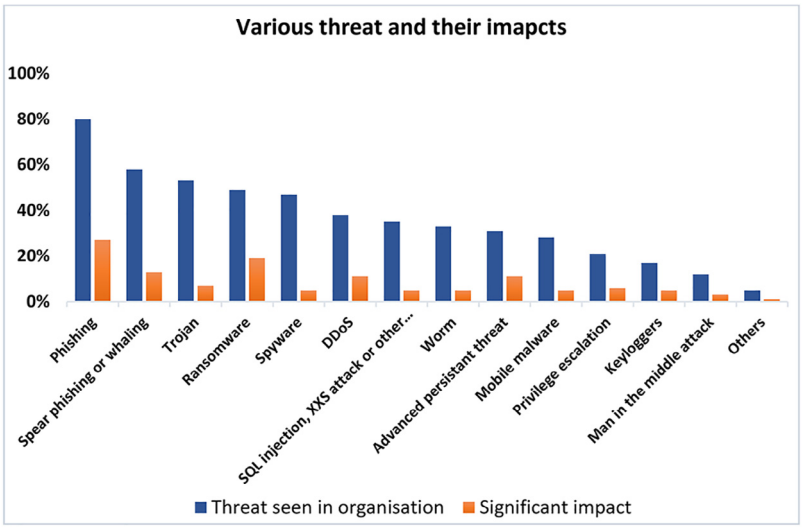

Fig. 3 – Threats and their impacts on organisations.

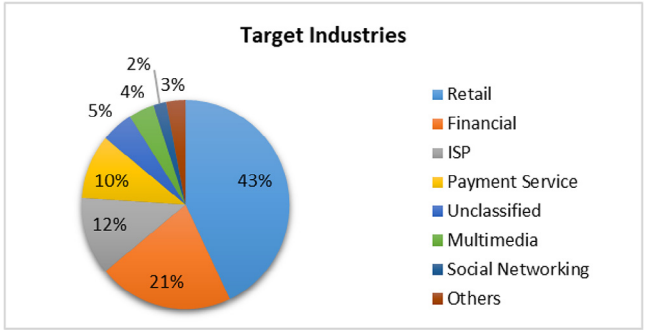

Fig. 4 – Industry sector targeted by mobile phishing attack (Phishingpro, 2017).

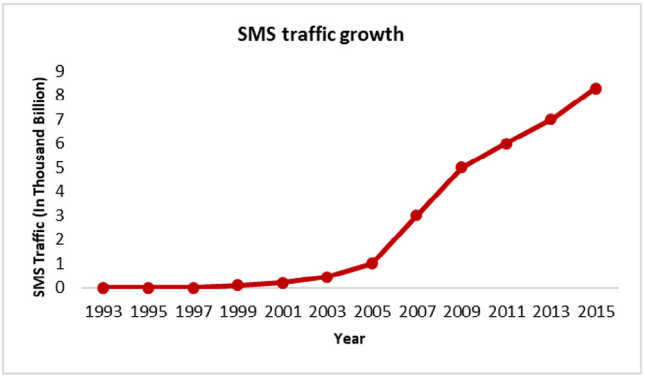

Fig. 5 – SMS traffic growth (1993–2015).

these messages, 17% of the users ignore them, 13% of the users answers with stop command and only 17% of the users report them (Mobile Ecosystem Forum, 2017).

Most targeted industry sector by mobile phishing attack is retail sector followed by financial, Internet service provider (ISP), Payment Services sector as shown in Fig. 4 (Phishingpro, 2017). According to Portio Research report (Statista, 2017b), SMS traffic increased to 100 billion in just 3 years from 1996 to 1999. By 2003, SMS traffic reached to 450 billion messages. In 2009, this traffic crossed 5 trillion and in 2015 it reached to 8.3 trillion as shown in Fig. 5. Fig. 6 illustrates trust level of user on different messaging platforms. 35% of the users consider SMS as one of the most trustworthy channel, 28% of the users trust various messaging applications like WhatsApp, Instagram, while 18% of the users trust messenger, Facebook, Yahoo and Skype (Mobile Ecosystem Forum, 2017).

According to PhishingPro report 2016 (Phishingpro, 2017), earlier 90% of successful phishing attacks begin with a phishing email. Attackers used spear phishing to target the users. But now attackers are using mobile applications instead of emails to gain credentials. In mobile phones, 81% of the phishing attacks are carried out using mobile applications, SMS, or

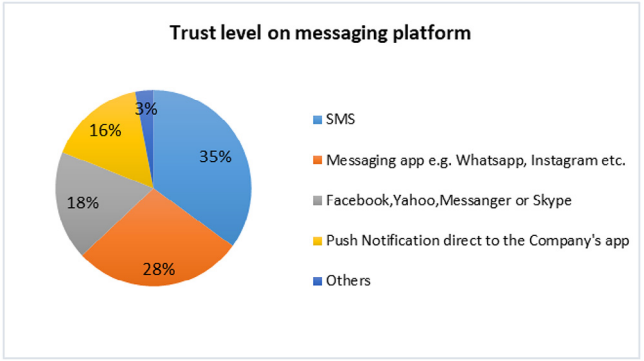

Fig. 6 – Statistics of trust level of user on various messaging platforms (Proofpoint, 2017).

websites while only 19% of the phishing attacks are carried out using mobile emails (Wandera, 2017).

Mobile applications are the frontline for the attackers to target users. According to Wandera report, 26% of Phishing attacks on mobile phone are distributed through gaming applications (Wandera, 2017). From all over the world, 1% of

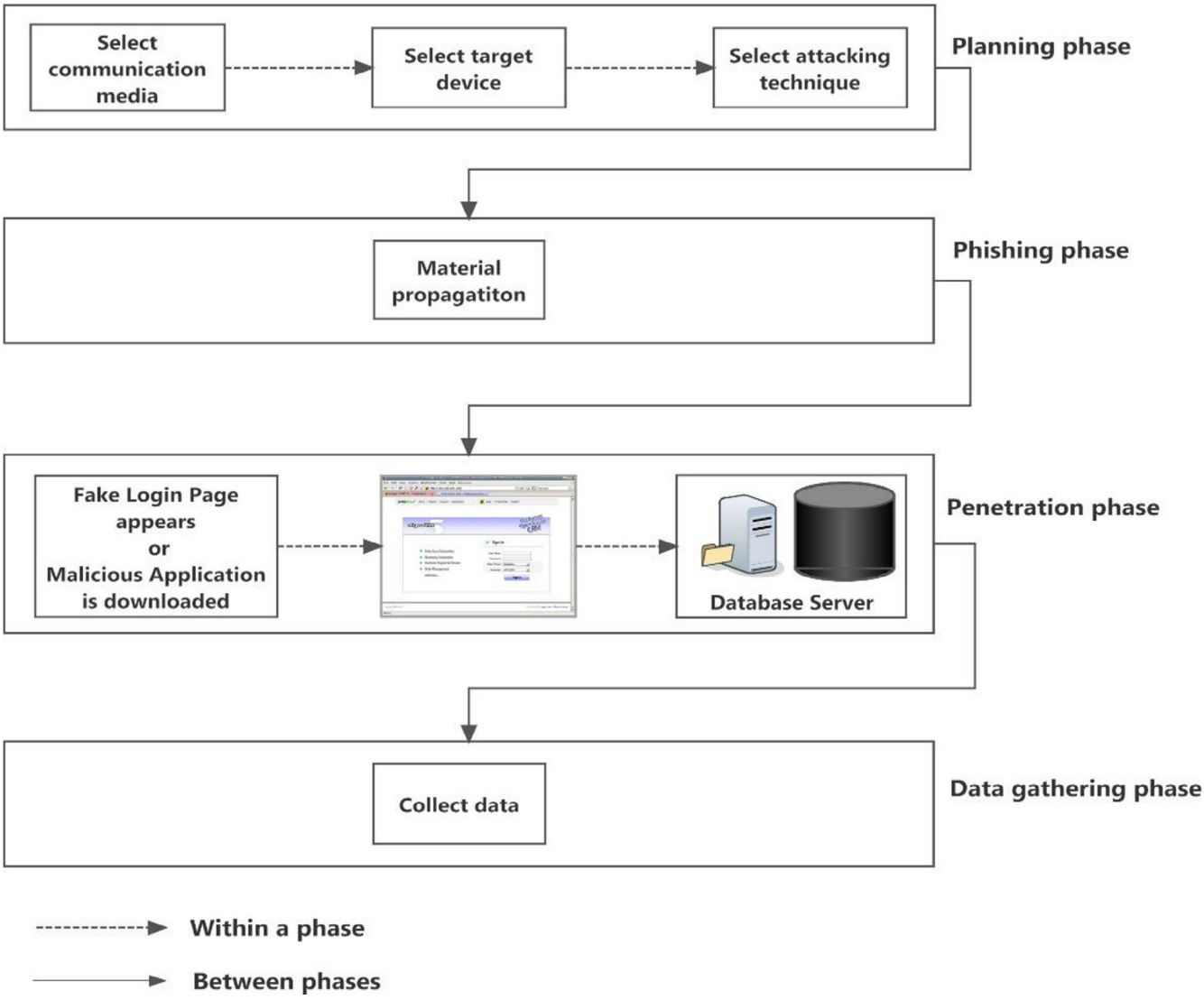

Fig. 7 – Mobile phishing life cycle.

application developers (approx. 16,000 publishers) are developing the malicious applications and distributing them through third party application store. Most of these applications masquerade as legitimate. From 2011 to 2013, the number of malicious applications held by Google Play Store has grown by 388%. In 2015, large number of applications was removed from Apple App Store and Google Play Store due to their malicious behaviour.

2.4. *Mobile phishing life cycle*

The following phases are involved in Mobile phishing attack [Fig. 7]:

Planning phase: In the first phase, the attacker selects a feasible communication media for initiating the phishing attack. This media can be a phishing webpage, a phishing application, an email, or an SMS containing a malicious link. The attacker sets the target that can be an individual, organisation, or a nation and collect details about them by physically visiting them or monitoring them. After that attacking technique is selected that can be malicious application, or SMS.

Phishing phase: In this phase, material is propagated to victim. The attacker sends phishing material to mobile device users using spoofed SMSes or emails pretending to be a legitimate source.

Penetration phase: Once the user opens the propagated material, either a login page appears which redirects user to a phishing webpage and asks for personal information, or a malicious application is downloaded, allowing the attacker to penetrate in the device.

Data gathering phase: As soon as the attacker gets access to the device, user's information is extracted either through the malicious application or fake login page. If a malware is installed in the device then the attacker can get remote access to the device and can get whatever information he wants from the device. Attackers can use gained information for financial benefits or other purposes.

3. Evaluation metrics and datasets

Evaluation matrices and datasets are used by many researchers for experimentation and evaluation of their proposed techniques. This section gives a brief description of various evaluation matrices and popular ham and spam datasets.

3.1. Evaluation metrics

In a binary classification problem, the objective is to identify the phishing instances from a set of phishing and legitimate instances. Here, four possibilities exist as shown in Table 2.

3.1.1. True Positive rate (TP)

It represents the rate of instances correctly detected as phishing with respect to all existing phishing instances.

$$TP = \frac{n_{P\to P}}{n_{P\to P} + n_{P\to L}} \tag{1}$$

3.1.2. False Positive rate (FP)

It represents the rate of instances improperly detected as phishing with respect to all existing legitimate instances.

$$FP = \frac{n_{L\to P}}{n_{L\to L} + n_{L\to P}} \tag{2}$$

3.1.3. True Negative rate (TN)

It represents the rate of instances correctly detected as legitimate with respect to all existing legitimate instances.

$$TN = \frac{n_{L\to L}}{n_{L\to L} + n_{L\to P}} \tag{3}$$

3.1.4. False Negative rate (FN)

It represents the rate of instances incorrectly detected as legitimate with respect to all existing phishing instances.

$$FN = \frac{n_{P\to L}}{n_{L\to P} + n_{P\to P}} \tag{4}$$

3.1.5. Precision (P)

It measures the rate of instances correctly detected as phishing with respect to all instances detected as phishing.

$$P = \frac{n_{P\to P}}{n_{L\to P} + n_{P\to P}} \tag{5}$$

Table 2 – Classification matrix.

	Classification	
	Phishing	Legitimate
Is Phishing	$n_{P\to P}$	$n_{P\to L}$
Is Legitimate	$n_{L\to P}$	$n_{L\to L}$

3.1.6. Recall (R)

It represents the rate of phishing instances correctly detected as phishing with respect to all existing phishing instances. It is same as TP.

$$R = \frac{n_{P\to P}}{n_{P\to P} + n_{P\to L}} \tag{6}$$

3.1.7. f_1 score (f_1)

It represents the harmonic mean between Precision and Recall.

$$f_1 = \frac{2PR}{P+R} \tag{7}$$

3.1.8. Accuracy (A)

It measures the overall rate of correct prediction.

$$A = \frac{n_{L\to L} + n_{P\to P}}{n_{L\to L} + n_{L\to P} + n_{P\to L} + n_{P\to P}} \tag{8}$$

Where:

$n_{P\to P}$ is the number of phishing instances correctly detected as phishing.
$n_{L\to P}$ is the number of legitimate instances incorrectly detected as phishing.
$n_{P\to L}$ is the number of phishing instances incorrectly detected as legitimate.
$n_{L\to L}$ is the number of legitimate instances correctly detected as legitimate.

3.2. Datasets

Availability of requested dataset is a major challenge faced by researchers while carrying out the research. Various datasets are available on the Internet that are used for research and assessment of phishing detection algorithms. Since the websites for mobile phones are not similar to their desktop counterparts, so there are some datasets available which provide ham and spam instances for desktop as well as mobile phones. In this section, we summarise datasets used by the researchers (Table 3).

3.2.1. SMS spam collection v.1

It is a public set of SMSes collected for SMS spam research. It has 5574 real text messages in the English language labelled as ham or spam (Department of Telematics, 2011). Out of 5574 SMSes, 425 spam messages are extracted from Grumbletext website, 3375 ham messages are randomly chosen from National University of Singapore (NUS) SMS Corpus (NSC), 450 ham messages gathered from Caroline Ph.D. thesis, rest of the 1002 ham and 322 spam messages are gathered from publicly available corpus.

3.2.2. The SMS spam corpus v.0.1 big

The SMS spam corpus v.0.1 big (Gomez Hidalgo, 2011) consists of 322 spam messages and 1002 ham messages in English language. It is freely available for use. The dataset consists of 202 ham messages from Jon Stevenson and some legitimate

Table 3 – Dataset description.

Dataset	Dataset type	Number of instances
SMS spam collection v.1 (Department of Telematics, 2011)	SMS	5574 text messages (747 spam and 4827 ham messages)
The SMS spam corpus v.0.1 big (Gomez Hidalgo, 2011)	SMS	322 spam and 1002 ham messages
DIT SMS spam dataset (Dublin Institute of Technology, 2012)	SMS	1353 spam text
Caroline Tag's PhD thesis (Tagg, 2009)	SMS	1002 ham, 322 spam text messages and additional 5574 English text messages
Deceptive opinion spam corpus (Ott)	SMS	1600 truthful and deceptive reviews
IronPorts (CISCO)	SMS and Email	Dynamic dataset
Enron email dataset (Enron Email Dataset, 2015)	Email	500,000 email
Spam email dataset (CSMINING Group, 2010)	Email	4327 emails for training and 4292 emails for testing
The 2005 TREC public spam corpus (Cormack and Programming Languages Group, 2017)	Email	39,399 ham emails and 52,790 spam emails
OpenPhish (OpenPhish)	Website	Dynamic dataset
Phishload (Phishload, 2012)	Website	More than 1000 legitimate websites
PhishTank (Phishtank, 2017)	Website	Dynamic dataset

messages from NUS SMS Corpus. The dataset also consists of 322 spam messages from Grumbletext site.

3.2.3. *DIT SMS spam dataset*

Dublin Institute of Technology (DIT) SMS spam dataset is a set of 1353 spam text SMSes collected from 2003 to 2010. SMSes are collected from two consumer complaints websites of UK and all text messages were received by mobile device users of UK. Each message has a date on which it was reported (Dublin Institute of Technology, 2012). This dataset is used by Delany et al. (Delany et al., 2012).

3.2.4. *Caroline Tag's PhD thesis*

Tag's PhD thesis named "A Corpus Linguistics Study of SMS Text Messaging" consists of SMS dataset gathered for carrying out research in SMS spam filter. It is publicly available dataset and consists of 450 ham SMS messages. It also contains 5574 English, non-encoded text SMS messages categorised as spam or non-spam (Tagg, 2009).

3.2.5. *Deceptive opinion spam corpus*

It is a collection of spam and non-spam review comments of about twenty hotels of Chicago. On the condition of proper acknowledgment of their source, the corpus is freely available for use. The corpus contains 1600 truthful and deceptive reviews from various Chicago hotels like TripAdvisor, Expedia, Hotels.com (Ott et al., 2011, 2013).

3.2.6. *IronPorts*

Scott Banister and Weiss designed IronPorts in 2000 and in 2007 Cisco acquired it (CISCO). It is a corpus of messages and emails submitted by consumers. Tyler Moore used IronPort corpus (Moore et al., 2009).

3.2.7. *Enron email dataset*

This corpus contains approximately 500,000 emails collected from 158 employees of Enron Corporation and later on, it was purchased by Leslie Kaelbling at Massachusetts Institute of Technology (MIT). This corpus was collected by A Cognitive Assistant that Learns and Organizes (CALO) project (Enron Email Dataset, 2015).

3.2.8. *Spam email dataset*

This dataset is suitable for spam filtering systems. Corpus contains 4327 training email messages out of which 2949 are ham messages and 1378 are spam messages. It contains 4292 email messages for testing, i.e. mails whose class label is unknown (CSMINING Group, 2010).

3.2.9. *The 2005 TREC public spam corpus*

It consists of 92,189 email messages labelled as ham or spam. Out of 92,189 emails, 39,399 are ham emails while 52,790 emails are spam emails (Cormack and Programming Languages Group, 2017). This corpus is freely available for use if used as per agreement.

3.2.10. *OpenPhish*

OpenPhish was launched in 2014 with an autonomous algorithm to detect zero-day phishing websites. It receives URLs and examines them with its phishing detection algorithm. If URL is categorised as Phish, Meta data associated with it is collected and feeds together with URL. The data is openly available at (OpenPhish).

3.2.11. *Phishload*

It contains a set of real phishing sites. Its database consists of HTML source code of phishing websites. It also contains more than 1000 legit websites. Three screenshots are taken from each website for detailed analysis (Phishload, 2012).

3.2.12. *PhishTank*

It is an Anti-phishing website and was launched in October 2006. PhishTank stores data and information of phishing websites as reported by the users. It is the largest clearing house of data related to phishing scams. It is used by Yahoo mail, Mozilla, Mcafee, APWG and many others. Data can be accessed using Application programming interface (API) or can be shared by the websites (Phishtank, 2017).

4. Security concerns of smartphones

This section discusses various security concerns related to smartphones that include assets of smartphone, security

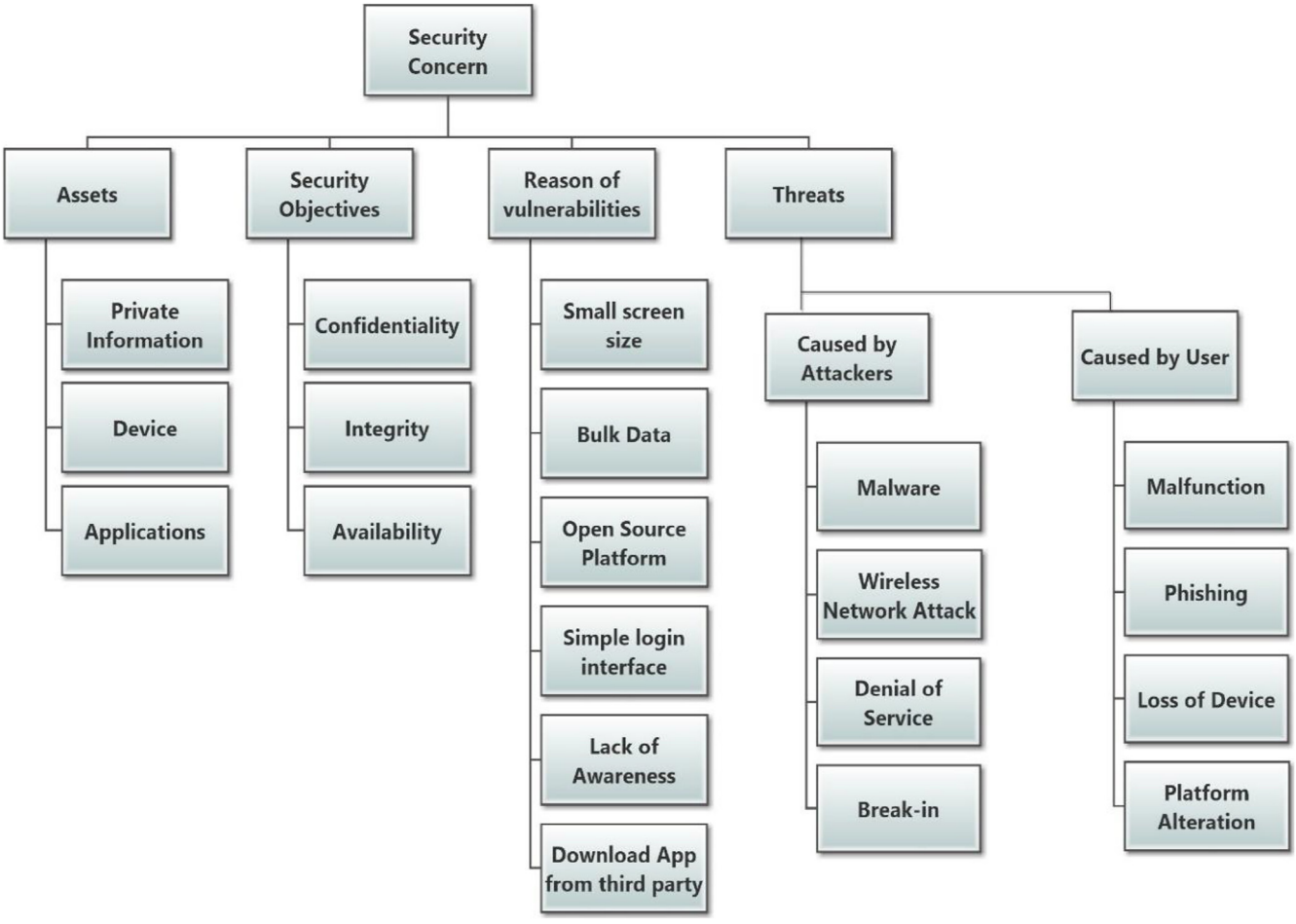

Fig. 8 – Security concerns of smartphones.

objectives, reason of smartphone vulnerability, and various threats to smartphones. Assets include resources of smartphones that encourage cybercriminals to initiate attacks on smartphone devices. Assets can be information, applications, or device itself. Smartphones should consider the security requirements like confidentiality, integrity, and availability. Vulnerabilities of smartphone let the attacker to gain access to the device. Threat can be caused by the attacker or by the user. Fig. 8 shows various security concerns of smartphones.

4.1. *Assets*

Attackers target the smartphones due to their assets, which can be private information, device itself, or applications installed on the smartphones. Information in the smartphone is an asset of device. It includes data stored in the device as well as data transmitted from the smartphone. For example, contacts, SMS, call history, location information, passwords used for login, and other information. Device itself is also an asset. Lost smartphone can be used by the attacker for carrying out malicious activities. Applications installed are also considered as an asset. Applications can be of two types, freely available applications and commercial applications, for which users have to pay some amount in order to use them. In order to avoid entering login information every time, users store their id and password on web browser or applications. So applications are closely associated with information (Jeon et al., 2011).

4.2. *Security objectives*

The security objectives of mobile devices include confidentiality, integrity and availability. Attackers violate these security objectives by attacking the devices. Confidentiality is one of the most important security objectives for establishing trust between sender and receiver. It determines who is authorised to access what. Integrity is when only authorised persons are allowed to modify or use the resources, and modification should be done in an authorised way. Integrity of information is protecting it from destruction and unauthorised modification. Availability means that the resources must be available to the legitimate users at any time and place of their requirements, with no delay.

4.3. *Reasons for smartphone vulnerabilities*

Researchers are working on security of smartphones, but are unable to analyse various security threats associated with the device. In order to establish security of the smartphones, vulnerabilities of smartphones need to be identified. Here, we have briefly described various reasons for smartphone vulnerabilities.

First is small screen size. With small screen size, it is hard to check the legitimacy of the page and full URLs are not displayed in the mobile browser. Second is bulk data. A significant amount of personal data is stored on the smartphones. Most of the users carry out their financial transactions, such as online shopping or banking transactions using smartphones, and this information is crucial. Attackers can have significant financial gains from this information. Third is open source platform. Most of the smartphones have open source platform such as Android. In Android, the kernel is open source due to which malware writers have a sound knowledge of the mobile platform which encourages them to develop and publish malicious applications. Users download and install applications, and the risk of introducing malware in the smartphones increases. Fourth is simple login interface. Usually mobile applications have simple user login interface which makes the task of developing a fake application or webpage easier for the attackers. Fifth is lack of user awareness. Users do not take the security of smartphones seriously either due to lack of knowledge or due to their irresponsible behaviour. Sixth is download applications from third party application store. Attackers use third party application store for spreading malicious programs. Applications that are freely available can be downloaded and installed by the smartphone users. Sometimes to trick the users, the attackers develop legitimate applications and release them on the play store. Then they modify the applications to include the malicious content and release an update (Parker et al., 2015).

4.4. *Threats to smartphones*

Threats to smartphones can be caused by the attackers or the users. Threats caused by the attackers can be malware threats that can expose or alter personal information stored in the smartphones, can affect the availability of the resources, and the functioning of the device. Wireless network attacks can corrupt, modify and block the data on the wireless networks by eavesdropping, spoofing or sniffing. Other threat is Denial of Service (DoS) attack which can risk the availability of the smartphone and its services to the user. Break-in threat is the threat in which an attacker can control the device partially or fully by injecting code, using flaws in the code or by abusing logical errors.

Threats caused by unawareness of the users are malfunctioning, phishing, loss of device or platform alteration. Inappropriate configuration by the users can cause malfunctioning of some of the applications. Due to incompatibility between applications and platform, smartphone applications may fail to function. Phishing is another threat caused by the careless behaviour of the user in which attacker obtain users personal information by tricking users. Loss of device is also a threat where attackers can use the device for malicious purposes (Jeon et al., 2011).

5. Taxonomy of mobile phishing attacks

The taxonomy of mobile phishing attacks is shown in Fig. 9. Mobile phishing attacks can be classified into various categories based on social engineering, mobile applications, malware, social networking sites, content injection techniques, or wireless mediums. Some of the mechanisms for carrying out phishing attacks on mobile phones are discussed below.

5.1. *Social engineering*

Social engineering is an art of deceiving users into disclosing their sensitive information. Instead of attacking the systems, social engineering attacks target the humans who have access to information and manipulate them into revealing their confidential information. In this attack, technical protection is not much effective as it targets the users and not their devices. In addition, people believe that they are smart enough and would not fall for such attacks (Yeboah-Boateng and Amanor, 2014). Social engineering attacks take advantage of ignorance and careless behaviour of users due to which sensitive information may be revealed. There are various social engineering approaches such as physical approach, social approach, reverse social engineering, technical approach, and socio-technical approach (Krombholz et al., 2015). Some of the social engineering methods for carrying out phishing attacks on mobile phones are discussed below.

5.1.1. *Phishing through SMSes*

One of the most popular methods to carry out phishing attacks on mobile phones is through SMS, and this method is called Smishing. This attack is intended to steal personal and financial information over the mobile phones. Smishing messages usually contain text message along with a link which when opened either redirects user to a fake website, or some malicious program is installed (Choudhary and Jain, 2017b). Through smishing, malware can enter the device. This attack is based on social engineering and users are easily targeted by it. Various methods have been proposed to detect malicious links included in the SMS but these links are changed frequently. Also URLs are shortened which makes it even more difficult to detect malicious URLs (Joo et al., 2017). Various reports clearly state that smishing attacks have exponentially increased over the past few years.

5.1.2. *Phishing through Voice over Internet Protocol (VoIP)*

Phishing over VoIP (Singh et al., 2014) has become very common and is also known by the name Vishing. Vishing is same as that of phishing and is carried out over phones using voice technology. Attackers gather information about the users, such as name, phone number, address, bank details and this is the information a genuine caller is expected to have. Moreover, users act without thinking during the phone calls (Infosec Institute, 2017). Attacker sets the target user as victim and makes him reveal his personal details. Vishing has a comparatively higher success rate than other mobile phishing methodologies because trust level that is built over the phone during the call is greater than other methodologies relying on the Internet (Lifewire, 2016).

5.1.3. *Website phishing*

In website phishing attack, attacker targets individuals instead of a system. It is very easy for an attacker to create an exact replica of a legitimate website. Attacker tries to trick users by

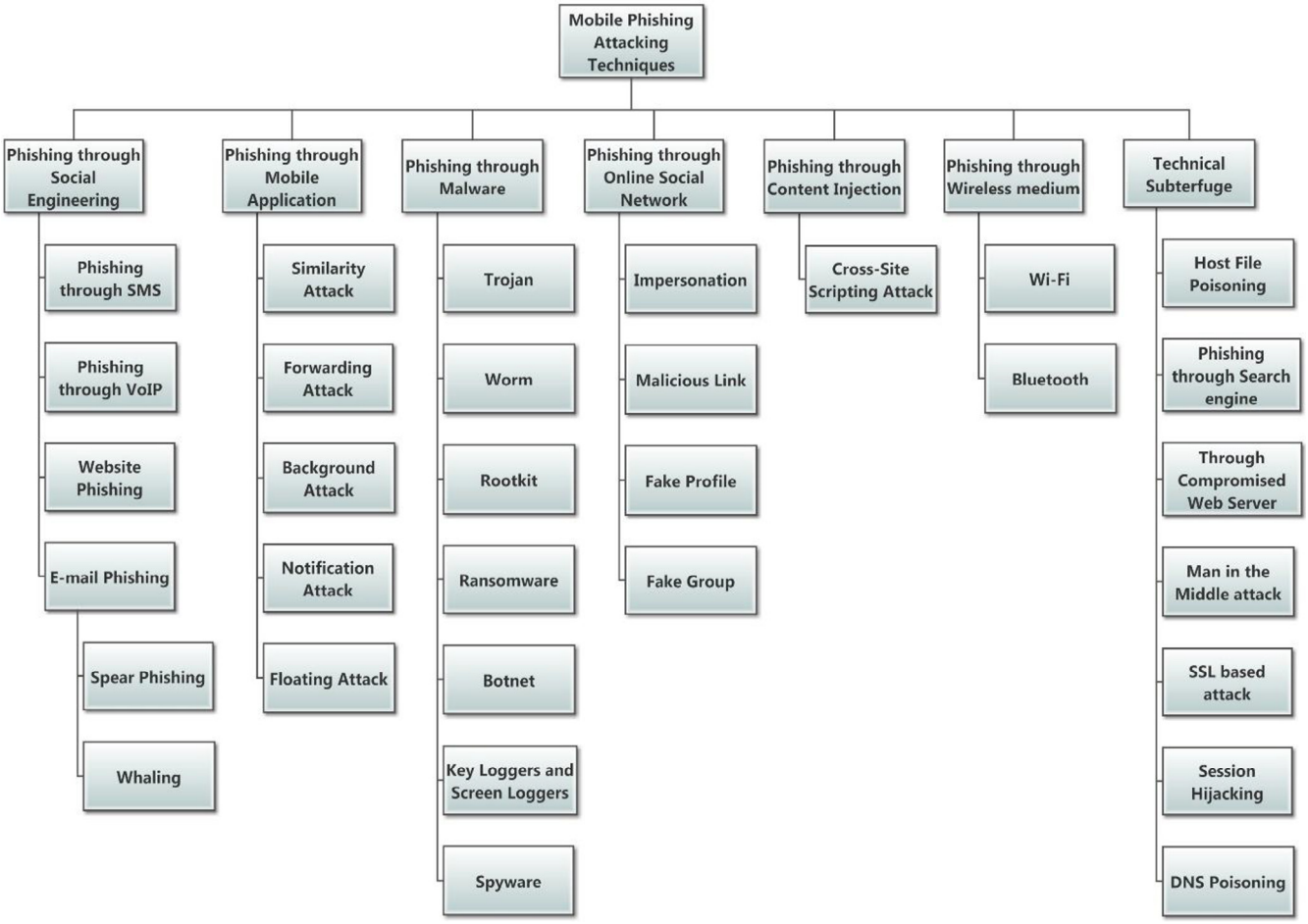

Fig. 9 – Taxonomy of mobile phishing attacks.

creating a phishing website of some famous websites, such as eBay, PayPal to obtain user's financial and personal details. A phishing website can be a legitimate website with phishing content inserted into it, or it can be a website owned by the phisher (Khonji et al., 2013). Blacklisting and heuristics based detection methods are used to detect phishing webpages. Blacklist contains suspicious IP addresses and URLs. In this approach, we search for the suspicious website in the list. Although it provides low false positive rate but does not protect from the Zero-Day phishing attacks. Heuristics methods are based on features which are present in most of the phishing webpages but not in all webpages. To bypass this, the attacker may design a website which may not have these features at all.

5.1.4. *Phishing through email*

Phishing email is a kind of spam message. These emails are illegal and rely on fake claims to be originating from legitimate company. The phisher sends a large number of fake emails along with a malicious link to users, requesting them to update their information in the provided link which when clicked either redirects user to a phishing website instead of legitimate one or ends up downloading a virus. Most of the approaches used to identify phishing emails are based on supervised, unsupervised and hybrid learning (Almomani et al., 2013). Many techniques have been developed to detect phishing emails, but still there is a lack of complete solution. Sequence diagram of mobile phishing through email is shown in Fig. 10.

5.1.4.1. *Spear phishing.* A new type of email phishing is spear phishing in which an attacker targets an individual, organisation or a business group (Hong, 2012). Spear phishing is effective as 70% of the users open these emails, and within an hour of receipt, 50% of them click on the link contained in the email (FireEye, 2017). In this attack, message appears to come from well known organisations or companies. Spear phishing attack is successful if the source of the message appears to be trustworthy, the information contained in the message support its validity and requests that the message contains seems to be logical (Search security, 2017).

5.1.4.2. *Whaling.* It is a kind of phishing scam that targets high profile companies or executives having valuable information. The target is chosen carefully according to the access and authority the person holds in the company. Attackers use social engineering to deceive users into disclosing their banking or personal details. Since these attacks do not use malicious URLs or attachments, these are difficult to detect (Mimecast, 2017). Since the profit amount that the attackers obtain from this attack is large, they spend comparatively more time and effort to make this attack successful (Digital Guardian, 2017).

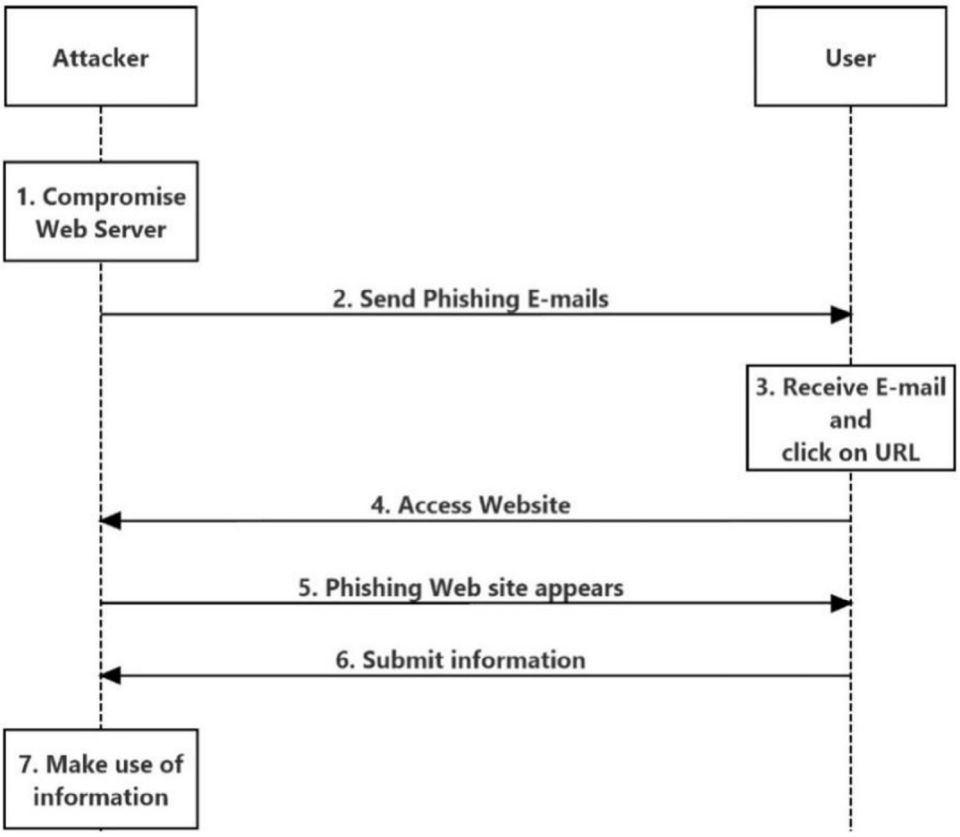

Fig. 10 – Sequence diagram of E-mail phishing.

5.2. *Phishing through mobile applications*

Application based phishing attacks are a major problem on the mobile devices. During browsing or downloading an application, a user may fall victim of phishing attacks. Once malicious applications enter the device, they collect personal information of user like login ids, passwords and transmit the same to the attacker. Attacker may install a backdoor and other application which can breach privacy of the user (Khurana et al., 2016). Fig. 11 shows the process of distribution of malicious applications in mobile phones. Small screen size and lack of security indicators makes it difficult to detect phishing attacks on mobile devices. Mobile application oriented phishing attack is classified into two categories: first, when phishing application tries to hijack existing legitimate application; second, when phishing application directly pretends to be a legitimate application. This happens when user downloads a fake application from an unauthorised application market (Wu et al., 2016). During installation, the application asks for various permissions that do not go with what the application is supposed to do (Proofpoint, 2017). Various phishing attacking techniques on mobile application are discussed below.

5.2.1. *Similarity attacks*

In similarity attack (Marforio et al., 2015), the phishing application, webpage or login interface have the same name, User

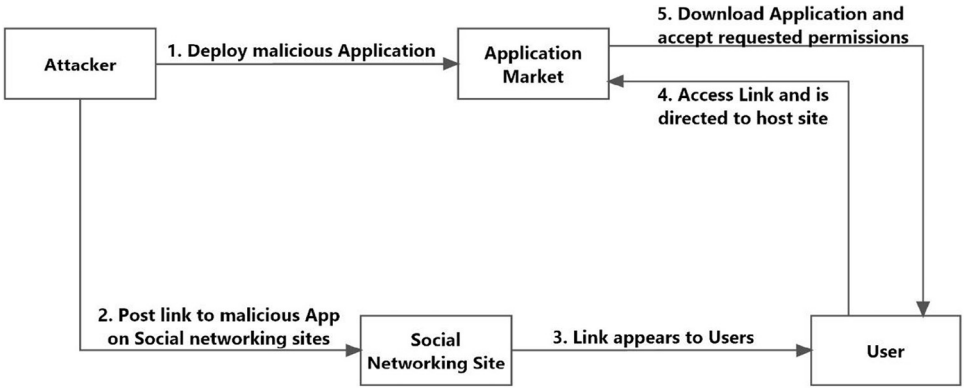

Fig. 11 – Distribution of Malicious Applications in Mobile phones.

interface (UI), and icon as that of the legitimate one. The attacker prompts the user to install phishing application and give login information in phishing Login User Interface (LUI) instead of legitimate one.

5.2.2. *Forwarding attacks*

Forwarding attack is a type of phishing technique. In this attack, a phishing resource encourages users to share his activities like high score in a game on social networking sites and requests to launch the social networking application. When the user clicks the button to launch the social networking application, instead of launching the social networking application, a phishing login page is displayed. The phishing page asks for the login credentials to access the account. These types of forwarding attacks are difficult to detect.

5.2.3. *Background attacks*

Sometimes the malware or the phishing application runs and wait in the background and use ActivityManager of Android, to keep track of other applications running on the device. Whenever the user initiates a genuine target application, the phishing application turns-on itself in the foreground, and phishing screen is displayed.

5.2.4. *Notification attacks*

The attacker might show a false notification asking the user for the personal details. The notification window can be modified by the attacker to look exactly like the genuine notification window.

5.2.5. *Floating attacks*

The attacker uses the feature of Android device that permits an application to draw some action on top of that application in the foreground. Phishing application having the SYSTEM ALERT WINDOW permission may show a see-through input field over the login id and the password input field of the genuine application (Marforio et al., 2015). The LUI of the genuine application is seen by the user, but the coated input field is not visible to the user. Whenever the user enters the credentials in the input field, credentials are received by the phishing application.

5.3. *Phishing through mobile malware*

The term "Malware" was first used in 1990, by computer scientist and researcher Yisrael Radai (Search security, 2016). Malware is a malicious software that gains access to device of the user without his consent. It is designed to steal data from the device, damage the device, or to annoy the user. Malware spreads via malicious attachments or malicious links. Attacker deceives user into installing malicious application and gain unauthorised access to the user's device. Malware secretly accesses personal data of the users and sends it to its host or attacker. Malware takes advantage of loopholes present in the operating system or browsers, to deceive users and encourage them to execute the code (Felt et al., 2011). In 2015, 430 million new unique malware were discovered by Symantec (Symantec, 2017a, 2017b). Table 4 shows various smartphone attacks, their effects and possible solutions.

Table 4 – Smartphone attack, their effects and solutions.

Attack	Effect	Solution
Trojan	Collect confidential information	Anti-virus and device specific intrusion detection system
Worm	Create backdoor for the attacker	Antivirus
Rootkit	Hide worms, bots and malware	Update device patches
Spyware	Collect confidential information	Firewall, Anti-spyware
Virus	Unusual behaviour of device	Antivirus
Backdoor	Effect security of device	Anti-virus and update device
Malware	Collect confidential information	Anti-virus and Malware detection system
XSS attack	Disclosure of sensitive information	Use of authorised apps

5.3.1. *Trojans*

By using various mobile applications attacker can gain control over the device. Such kinds of applications appear to perform some useful functionality in the foreground but perform malicious actions in background. Attackers can use Trojan to collect private information or for installing malicious applications like bots, or worms in the device. For example, a fake banking application can collect login information from the user. These applications mainly spread through third party application store (Delac et al., 2011). Trojan can create a backdoor and spy on the device, turning the device into a zombie, or can use it to send costly messages.

5.3.2. *Worms*

Worm is a malicious self-replicating application that can spread into uninfected systems by itself without human intervention. For propagation, worm relies on vulnerabilities of networking protocols. Due to its replicating nature and capability to spread itself over the network, it damages and affects the security of the device and consumes the bandwidth of the network. With the introduction of Cabir, malware can be ported to the mobile devices. Cabir (Dunham, 2008) worm attacks Symbian S60 devices, and it spreads through Bluetooth. Worm is observed only when its replicated instances consume system resources making the device slower.

5.3.3. *Rootkits*

It is a malicious application that runs under the privileged mode. Rootkit works in such a way that the user is not aware about the fact that operating system has been compromised. Rootkit itself is not harmful but is used by attackers to hide worms, bots and malware. It is not used to get access to the device but to hide malware efficiently (Landman, 2010). During installing a rootkit, attacker has to get access to root account either using social engineering or by cracking the password. Since rootkits are initiated even before the operating system of the device, these are difficult to detect and remove (Nortan, 2017).

5.3.4. *Mobile ransomware*

It is a malware that locks the device of the user preventing him from accessing the data. Ransomware encrypts the data of in-

Table 5 – Top 10 countries attacked by ransomware.

Rank	Country
1	USA
2	Japan
3	UK
4	Italy
5	Germany
6	Russia
7	Canada
8	Australia
9	India
10	Netherlands

fected system and decrypts the data only when ransom is paid to attacker. Ransomware attacks both computer as well as mobile phones. It locks the phone by changing the PIN number and then asks for ransom to unlock it. Ransomware can be of two types – crypto ransomware and locker ransomware. Crypto ransomware encrypts the file and data while locker ransomware locks the devices so that the owner of the device can not access the data. Most of the ransomwares declare their presence in the devices so as to collect ransom from the owner (Richardson and North, 2017). Table 5 shows the top 10 countries attacked by Ransomware (Richardson and North, 2017).

5.3.5. *Botnets*

Botnet is a network of compromised computers called "Zombies", in which a malware called bot is installed in the device by the attacker. Main goal of this strategy is to utilise the computational power of the compromised machines to commit other activities. These compromised machines after installation of the malware into them are controlled by the attacker from remote locations. These devices are used to send a large number of spam emails, information theft, and can also be used to launch DDoS attacks. Most of the bots are developed by the attackers for financial gains (Delac et al., 2011).

5.3.6. *Key loggers and screen loggers*

Key loggers and screen loggers when installed in the device can cause a serious threat to it. They are distributed as malware and are not detected by anti-viral software. Key logger records the key pressed by the user with a keyboard of the compromised device and sends this recorded data to the attacker without user's knowledge. Screen logger records the screen and the mouse movement, thus making use of virtual keyboard unsafe.

5.3.7. *Spyware*

Attacker uses online available spyware to take over the mobile phone, with which they can control SMS, emails, listen to phone calls, and track victim's position using GPS. Concealed channels present in the smartphone are used by spyware for sending information to the attacker. When an application needs to send data to the outside world for legitimate purpose, the permission settings of the smartphones are not strict enough to prevent misuse of such authorization for any other purpose (He et al., 2015). Zitmo spyware is one of the most dangerous spyware.

5.4. *Phishing through online social networks*

For both professional as well as personal communication, social networking sites are used by millions of people around the world and have become an important part of the Internet. Social networking sites allow users to interact and share their ideas with other users. As large numbers of people are the part of these networking sites, it is a new ground of attacks for the attackers. Attackers exploit user's trust on social networking sites for their own benefits (Symantec, 2017a, 2017b). Some examples of social networking sites are Facebook, Twitter and MySpace. In 2016, phishing attacks on social media have increased by 150% (Proofpoint, 2017). Attackers are using social networking sites to initiate phishing attacks due to the popularity of these sites, and it is somewhat easy for an attacker to masquerade as someone else on these sites. 24% of the users click on fake social media connecting requests and half of these users even share their credentials (Wandera, 2017). The study shows that it is easy to trick the people on social networking sites. Also, Internet users are four times more likely to become a victim especially if they are asked by the person who claims to be their known. Various methods with which attackers can deceive users on social networking sites are discussed below.

5.4.1. *Impersonation*

Users like to follow the famous personalities on social networking sites and join groups of their interest. There is no procedure that verifies whether a virtual profile is actual or not (Symantec, 2017a, 2017b). The attacker makes use of this and pretends to be a famous personality and posts some malicious links regarding sale or offers which if opened, ask for personal details or end up downloading a malware (Advantis, 2017).

5.4.2. *Posting malicious links*

Attackers use malicious links to redirect the user to some external malicious website which is under the control of the attacker. The links may be posted by dummy accounts. When a malicious URL is posted by the attacker, nearly 90% of the clicks occur within 24 hours after they are posted (Proofpoint, 2017). The redirection can be accomplished by social engineering where link appears to be a promising link. It is difficult for social media provider to block social engineering attacks as it is difficult to identify if it is legitimate or not. The redirected website may contain misleading information like malicious application, fake login page, or advertising fake products (Symantec 2017a, 2017b).

5.4.3. *Fake profiles*

Attacker may send friend request to the users claiming to be their old friend. Once added to the friend list, attacker can access private information which the user shares with his friends, family and colleagues. For more information, attacker may inbox user asking for phone number or email (Infosec institute, 2017).

5.4.4. *Fake communities*

Attacker may create a fake group with the name of well known organisation and add some members to the group who are

already the part of that organisation but are also with the attacker to carry out the scam. They send group request to other members of the organisation who after seeing that their colleagues are also the members of the group, join the group. Attacker then obtains the secret information from their discussions and uses it for his personal gain.

5.5. *Phishing through content injection*

In this, phisher modifies part of the content of the reliable website to deceive the user and takes him out of the legitimate webpage where he is asked for the personal information. For instance, an attacker may inject malicious code to record user's information and deliver it to the attacker's server.

5.5.1. *Cross site scripting (XSS)*

XSS attack is an application layer web attack that targets vulnerable scripts embedded in the webpages that are executed on client side. JavaScript is used to deliver the malicious content to the users and alters the client-side scripts of the web application so that the script executes as per the attacker. XSS attacks have severe effects and results in compromise of user's account, modification of content of webpage, and revealing the credentials or session cookies (Imperva, 2017).

5.6. *Phishing through wireless medium*

5.6.1. Wi-Fi

Wi-Fi has become a vital part of our generation and as a result, hotspot for the attacker. Generally users do not authenticate the access point to which they are connecting and it is not difficult for an attacker to set up a bogus access point with Service Set Identifier (SSID) which looks similar to the legitimate one. Attacker can interrupt communication between mobile phone and the Wi-Fi hotspot (AUJAS, 2015). Hotspot architecture is vulnerable, and it does not perform any encryption to protect the data being transferred. When the user connects to this type of hotspot for the first time, the connection between the two is not secure, and the attacker can interrupt and control the traffic, thereby hijacking the session.

5.6.2. *Bluetooth*

Bluetooth is a technology standard with which data can be shared over wireless links among the devices which are present within a short range. Devices having Bluetooth have some flaws due to which others can connect to the device without user's permission (AUJAS, 2015). When the two mobile devices are in the range of each other, attacker's mobile device can send malicious data to the victim's device by establishing a Bluetooth connection using default Bluetooth passwords (Delac et al., 2011). Once attacker gains access to the device via Bluetooth, contacts, messages, and files can be accessed by him.

5.7. *Technical subterfuge*

It is a method of tricking users in order to get some information that can be used by attackers for personal benefits (Gupta et al., 2017). Mobile phishing attacks based on technical subterfuge are discussed below.

5.7.1. *Host file poisoning*

A host file is the one which contains domain names and their corresponding IP addresses. When a client requests for a URL, it is first converted into IP address before transmitting it over the Internet. Host file poisoning involves altering the entries of the website in host file so that the user is redirected to a fraud website where the user is asked for the personal information (PCWorld, 2017).

5.7.2. *Phishing through search engines*

Phishing attack also makes use of search engine that redirects the user to online shopping websites that offer services or products at low price. When the user tries to buy the product, the website collects the credit card details. Here the search engine is legitimate, but the website is fake, which is created by the attacker to steal personal information. The search engine may show discount offers, job offers, etc. to lure the victim (PHISHING. org, 2017).

5.7.3. *Using compromised web servers*

Attacker looks for the vulnerable web server, and then compromises these servers. Password protected backdoors are installed and attacker gains access to the server via encrypted backdoor. Pre-built phishing websites are downloaded and with the help of mass email tools, fake websites are advertised (The Honeynet, 2008).

5.7.4. *Man-in-the-middle (MITM) attack*

In this attack, attacker sits between the victim and the legitimate website. The data submitted to the legitimate website is received by the attacker which can be credit card details or any personal information. The attacker continues to pass the data to the legitimate website so that user's transaction is not affected. Secure Socket Layer (SSL) traffic is not vulnerable to MITM attack (Bicakci et al., 2014), but a malware based attack can modify the system configuration for installing a trusted certificate authority through which attacker can create his own certificate.

5.7.5. *Secure Socket Layer (SSL) based attacks*

Phishing attack is carried out through untrusted websites. Though phishing website and original website look similar, the difference is that phishing websites do not have SSL certificate. SSL certificate is used by website operator to ensure data is transmitted over secure channels between browser and server. Phishing websites do not use SSL certificate based communication. Moreover after getting the credentials, phishing website may redirect user to original website having SSL certificate to fool users (Shahriar and Zulkernine, 2010).

5.7.6. *Session hijacking*

Session hijacking is exploiting valid computer session of the user. In this attack, attacker tries to obtain session id of the user in order to hijack the user's account. When a user submits his credentials, application server tries to authenticate him on the basis of the cookie values which consist of session id (SID). So if the attacker gets SID of an active user, he can use it and login to the account, and gets access to details available in the account (Infosec institute, 2015).

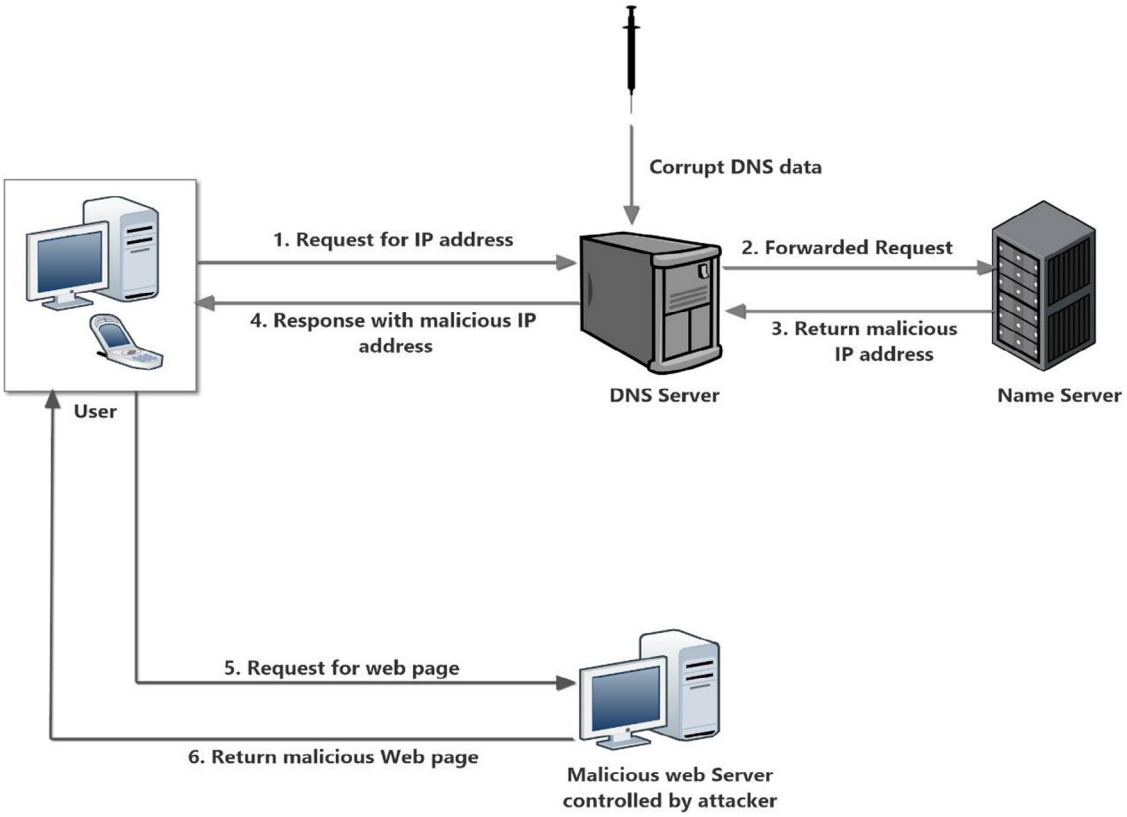

Fig. 12 – Phishing through DNS poisoning.

5.7.7. *Domain Name Server (DNS) poisoning*

It is a type of attack in which an attacker takes advantage of vulnerabilities present in domain name server to divert the incoming legitimate traffic towards the fake websites (Abu-Nimeh and Nair, 2008). Whenever client browser requests for a domain name, the request is sent to the DNS server for getting corresponding IP address. Attacker can set up a fake DNS server or alter the existing DNS table, changing the IP address corresponding to the domain name. Once the DNS is poisoned or fake entries are created, users are redirected to spoofed webpages (How-To Geek, 2016). Fig. 12 shows process of phishing through DNS poisoning.

6. Taxonomy of mobile phishing defence mechanisms

In this section, various approaches for detecting and defending against phishing attacks on mobile phones are discussed. Comparative analysis of various mobile phishing defence techniques is shown in Table 6. Anti-phishing solutions for various mobile phishing attacks are presented in Table 7.

6.1. *User education*

Phishing is one of the most significant problems faced by Internet users. User education is important in order to create awareness among the users about phishing attacks. Phishing is a social engineering attack. Hence, educating the user is important to avoid phishing attack. Education based approaches include showing warnings, and online training through games.

6.1.1. *Active and passive warnings*

User interface shows warning depending upon the action triggered as deployed by many web browsers. The warning can be a passive warning that only shows the warning and relies on the users to perform certain action while active warning does not rely on the user to perform some action and block the content itself. Users do not pay attention to the warnings. Studies have shown that passive warnings are less effective as compared to active warnings.

6.1.2. *Training through mobile games*

One of the important factors in avoiding phishing attack is to train users which leads to correct identification of phishing and legitimate instances. Various methods are there to train the users. To develop conceptual knowledge about phishing attacks, various mobile games are being developed to educate the users. With the increase in use of Internet technology, the risk of mobile device users falling victim to phishing attacks have also increased. So mobile games can be used to train the users which further helps in reducing the phishing threat. Asanka et al. (2012) designed one such game. The game is about educating the users about phishing emails and phishing URLs so that the user is able to differentiate between phishing and legitimate emails and URLs. The prototype of the game was implemented on Google App Inventor Emulator. In another approach,

Table 6 – Comparisons of various existing solutions for mobile phishing.

Approach	Techniques	Specific for	Advantages
kAYO (Amrutkar et al., 2017)	Machine Learning	Mobile Webpages	90% classification accuracy, 89% true positive rate, 8% false positive rate.
MobiFish (Wu et al., 2016)	Optical character recognition	Mobile webpage, application, and persistent account.	Web-Fish achieves 100% verification rate.
Chorghe and Shekokar (2016a)	SVM classifier and URL based heuristics	Mobile Webpages	92% accuracy and protects from zero-day phishing attacks.
Tripathi and Gangwani (2017)	Machine Learning	Mobile Webpages	High classification accuracy; browser extension for real-time feedback
Mukhopadhyay and Argles (2011)	Mobile QR code	Webpage authentication scheme	Protect against man in the middle attack and replay attacks.
Choi et al. (2011)	Mobile QR code	Webpage authentication scheme	Data is encrypted so credentials are safe even if attacker obtain them; user can check if server is phishing or not.
MP-Shield (Bottazzi et al., 2015)	Blacklist and data mining approach	Mobile Webpages	Ensure zero-hour protection; Protect android devices from phishing attack.
El-Alfy et al. (El-Alfy and AlHasan, 2016).	Dendritic cell algorithm	Emails and SMS	The dendritic cell algorithm improves recall and precision of spam and non-spam messages; accuracy approx. 100%.
S-Detector (Joo et al., 2017)	Naive Bayes classifier	SMS	Approach is able to detect and block smishing messages with high accuracy rate.
MDLText (Silva et al., 2017)	Minimum description length principle	SMS	Able to process high dimensional data at fast speed; Low computational cost.
SMSAssassin (Yadav et al., 2011)	Bayesian learning and sender blacklisting mechanism	SMS	72.5% and 97% classification accuracy in spam andnon-spam messages respectively.
Almeida et al. (2016)	Text processing with lexicographic and semantic dictionaries	SMS	For the Wilcoxon Signed-Ranks Test, the null hypothesis is rejected with $\alpha = 0.05$ with a confidence level of 95%.
Canbay et al. (2017)	J48 classification and K-Means clustering algorithm	Mobile Application	Approach can detect malign and benign applications with 98.6% accuracy.
VeriUI (Liu and Cox, 2014)	augments user's credentials with hardware and software information	Mobile Application	Prevent phishing attacks through secure, hardware isolated environment for password input and transmission.

Table 7 – Anti-phishing solution for various Phishing techniques.

Phishing Techniques	Anti-Phishing Solution
Smishing	Dynamic models and framework Blacklist
Vishing	User training Blacklist
Phishing websites	Password management tools Trusted path ensured browser Client server authentication Browser extension Pattern matching Blacklist
Phishing and spam emails	Anti-spam filters Client server authentication User training
Phishing applications	Personalized security indicators Permission based analysis
Malware	Anti-malicious programs

Arachchilage et al. (Arachchilage and Love, 2013) developed a game by identifying the elements that are needed to be addressed to avoid phishing attacks for educating users. In addition, Asanka et al (Arachchilage and Hameed, 2017) designed a gaming approach by combining conceptual and procedural knowledge to educate users. The approach integrates "self-efficiency" to the anti-phishing educational game in order to enhance user's behaviour to avoid phishing attacks. Other game based approaches are presented in Arachchilage and Cole (2011, 2016), Arachchilage et al. (2015) and Yang et al. (2017).

6.2. *Detection of smishing and spam SMSes*

Smishing messages consist of a text message and a URL which when opened perform malicious activity. Attackers use social engineering approach to target victims and users are easily attacked by it. For detecting smishing or spam messages, different classifiers that make use of effective feature set are used. Table 8 shows the comparative analysis of various smishing detection approaches. Various approaches for detecting smishing and spam messages are discussed below.

6.2.1. *S-Detector*

Joo et al. (2017) proposed a security model "S Detector" for detecting and blocking smishing messages. Naïve Bayesian Classifier is used to differentiate between smishing and normal messages by extracting the words most often used in smishing messages. S-Detector consists of four components – SMS monitor, SMS determinant, SMS analyser, and Database.

S-Detector takes the following steps to distinguish normal messages from Smishing messages.

Table 8 – Comparison of various smishing detection approaches.

Security features	Joo et al (Joo et al., 2017).	Yadav et al (Yadav et al., 2011).	Lee et al (Lee et al., 2016).	Smishing defender (Hauri, 2016)
Check for presence of URL	✓	x	✓	✓
Check for APK download	✓	x	✓	✓
Check for login page	x	x	x	x
Check for sender's mobile number	✓	✓	✓	✓
Check for self-answering messages	x	x	x	x
Text normalization	x	x	x	x
Content based analysis	✓	✓	✓	✓

Table 9 – List of features for detecting spam messages (Adewole et al., 2017).

S. No.	Feature	Description
1	No. of characters in message	Length of message on basis of number of characters
2	No. of words in message	Length of message on basis of number of words
3	Frequency of word "money"	Number of times word "money" appears in message
4	Frequency of symbol "money"	Number of times symbol "money" appears in message
5	Words in capital letters	Count the number of words that appears in capital letters
6	Number of special character	Number of special character appears in message
7	Number of emoticon symbol	Number of times emotional symbol appears in message, generally used by legitimate user
8	Presence of links	Check for the presence of link in message, mostly used by attackers
9	Presence of phone number	Check for the presence of Phone number in message, generally used by attackers
10	Average number of words	Ratio of number of words to number of characters in message
11	Number of sentence	total number of sentence present in message, sentence tokenizer can be used

1) When a text message is received, SMS monitor records the logs and timestamps of the communicated SMS message.
2) It is checked if the telephone number is already registered in blacklist database.
3) It is determined if the text message contains a URL. If yes, accesses that URL.
4) It is checked if an APK file is downloaded on access to the URL. If an APK file is downloaded, it is regarded as smishing message and is blocked, else content of the message is analysed.
5) Pre-processing is done to separate the strings from the text message and morpheme unit are extracted. Then a weight value is assigned to each word using Naïve Bayes algorithm.
6) If weight is more than or same as threshold, the message is labelled as a Smishing message and is blocked. Otherwise, it is categorised as a normal message.

6.2.2. *SMSAssassin*

Yadav et al. (2011) proposed a mobile spam messages filtering application "SMSAssassin" based on Bayesian learning. Support Vector Machine (SVM) is used along with Bayesian learning in order to achieve higher accuracy. Spam SMS consist of patterns and keywords that are changed frequently. Crowd-sourcing is used to keep the list of patterns updated. During the training stage, the occurrence of each word in spam and ham messages is computed to determine whether a word belongs to ham or spam. After training, the spaminess probability of SMS is calculated, and if it is above a certain threshold, then it is regarded as spam message. To keep track of spam keywords, SMSAssassin uses GlobalSpamKeywords at the server and SpamKeywordsFreq list in mobile phones. The mobile application also maintains a UserPreferencesList under which user can mention ham/spam keywords according to his choice or preferences. Users having SMSAssassin application in their mobile phones can share reported spam list. Authors collected a total of 4318 SMSes using crowdsourcing. Bayesian learning technique gives 97% classification accuracy in ham SMSes, 72.5% classification accuracy in spam. Table 9 shows the list of effective features for detecting spam messages.

6.2.3. *Dendritic Cell Algorithm (DCA) based approach*

El-Alfy and AlHasan, (2016) proposed a technique for filtering multimodal textual messages including emails and short messages. Inspired from the human immune system and hybrid machine learning methodologies, the author proposed a method for information fusion. Various features obtained from the received messages were analysed with the help of machine learning algorithm. They developed a framework based on DCA for mobile spam filtering by fusing output from machine learning algorithms.

6.2.4. *Text normalization and semantic indexing based approach*

Almeida et al. (2016) proposed a mechanism that normalises and expands the short and noisy text messages. Semantic and lexicographic dictionaries are used for this purpose. The text is processed in three stages: text normalization, concept generation, word sense dis-ambiguity. Text normalization normalizes and translates each term into its canonical form and uses two dictionaries – first is English dictionary and second is lingo dictionary. Concept generation is used to obtain every meaning or concept related to a particular term. Word sense dis-ambiguity is used to find the most relevant concept or meaning according to the context of the message. Concept generation and word sense dis-ambiguity uses LDB BabelNet

Repository. Authors concluded that with the help of text processing, classification performance can be enhanced. The system improves the quality of the attributes obtained, which in turn improves the classification accuracy.

6.2.5. *Spam detection using text content*

Karami and Zhou (2014) proposed a content based approach which instead of depending on individual word, uses a semantic group of words as features. Linguistic Inquiry and Word Count (LIWC) and SMS Specific (SMSS) features are the two semantic categories of features used by the researchers that help to reduce the feature set, in turn improving the efficiency of the approach. There are two phases in the system – feature extraction and classification. Machine learning algorithm is used for classification. Accuracy of the system lies from 92% to 98%.

6.2.6. *Smishing defender*

An application "Smishing defender" was developed by Hauri Inc. that detects and blocks phishing SMS messages in Android smartphones. The application monitors the text messages received and notifies the user on the reception of smishing message. The application also provides a feature with which suspicious message can be sent to Hauri for further analysis (Hauri, 2016).

6.2.7. *MDLText based approach*

Increasing volume of data in smartphone devices requires efficient and effective text classification methods. Silva et al. (2017) developed "MDLText" which is an efficient, scalable, fast, and lightweight multinomial text classifier based on the Minimum Description Length principle. MDLText is robust, learns faster and avoids over-fitting problem. Due to incremental learning, the scheme can be used in online as well as dynamic scenarios. Even with large volume of data, MDLText has lower computational cost.

6.2.8. *Detecting smishing in cloud computing environments*

Lee et al. (2016) proposed a technique to detect smishing messages using cloud virtual environment. The proposed technique checks for source of the message, content and location of the server and takes decision accordingly. Smishing detection probability is increased by using program interface analysis and filtering so as to minimize incorrect detection. On receiving a message, the user can compute the risk of the message in virtual environment and processing is also done there. When the process is completed, the screenshot and the report are sent to the user. Based on the report, user can determine if the message is smishing or not which in turn reduces the incomplete and false detection.

6.2.9. *Feature based framework for SMS Spam Filtering*

Uysal et al. (2012) proposed a framework for SMS spam filtering. To find various features of SMS, it uses two feature selection methods that are based on chi-square (CHI2) matrices and information gain (IG). Features are fed to the Bayesian classifier to classify the SMS as ham or spam. The scheme was designed for android mobile phone users and evaluated on large set of SMSes including legitimate and spam messages and output shows that system gives accurate results in detecting both ham as well as spam messages. Feature selection process is discussed below.

CHI2 is deviation of expected counts from the observed counts and is computed as:

$$CHI2(t,c) = \sum_{t\in\{0,1\}} \sum_{c\in\{0,1\}} \frac{(N_{t,c} - E_{t,c})^2}{E_{t,c}} \tag{9}$$

where N is observed frequency, E is expected frequency for each term t and class c.

IG calculates the contribution that a term makes by its presence or absence and is calculated as:

$$\begin{aligned} IG(t) = &-\sum_{i=1}^{M} P(c_i)\log P(c_i) + P(t)\sum_{i=1}^{M} P(c_i|t)\log P(c_i|t) \\ &+ P(\bar{t})\sum_{i=1}^{M} P(c_i|\bar{t})\log P(c_i|\bar{t}) \end{aligned} \tag{10}$$

where M is number of classes, $P(c_i)$ is probability of class, $P(t)$ and $P(\bar{t})$ are presence and absence probability of term t, $P(c_i|t)$ and $P(c_i|\bar{t})$ are probability of class c_i, given the presence and absence of term t.

Probability of class C_i (where i = spam or legitimate) given SMS represented with feature vector X is calculated as:

$$P(C_i|X) = \sum_{j=1}^{n} \begin{cases} wD_{ij}, \text{ if } jth \text{ term occurs in SMS message} \\ -D_{ij}, \text{ otherwise} \end{cases} \tag{11}$$

where D_{ij} is the ratio of number of SMS messages in class C_i having jth term to the total number of messages in class C_i, n is size of feature vector, and w is weight value.

If the probabilistic model takes the frequencies of terms containing the feature vector into concern rather than presence of the term, the probability is calculated as:

$$P(C_i|X) = \sum_{j=1}^{n} \begin{cases} wD_{ij}T_j \text{ if } jth \text{ term occurs in SMS message} \\ -D_{ij}, \text{ otherwise} \end{cases} \tag{12}$$

where T_j is the number of occurrences of the jth term within the respective SMS message.

6.3. *Detection of phishing webpages*

Website phishing attack targets the users instead of systems and it is comparatively easy to carry out these attacks as creating an exact replica of a website is not a difficult task. Phishing websites are difficult to detect due to high level of similarity they possess with legitimate websites. So some techniques are required for detecting website phishing attacks. Some of the existing methods are discussed below.

6.3.1. *MobiFish*

Wu et al. (2014, 2016) proposed a lightweight anti-phishing scheme "MobiFish" for mobile platforms that protects users from phishing attack on mobile applications, webpages, and persistent accounts. The fundamental idea behind this scheme is that if there is any dissimilarity between the identity an instance actually is and the identity it claims to be then it leads to a phishing problem. The claimed identity is obtained from the screen presented to the user. Screenshot of the login screen is taken and Optical character recognition (OCR) tool is used

Table 10 – List of effective features for webpage (Amrutkar et al., 2017).

Type	Features
JavaScript based features	Presence of JavaScript, internal JavaScript, embedded JavaScript, external JavaScript, noscript; number of JavaScript, external JavaScript, internal JavaScript, embedded JavaScript, noscript
HTML based features	Presence of images, internal and external links; number of images, external links, internal links, Number of HTTPOnly cookies, number of cookies from header, presence of iframes and redirections, whether webpage served over Secure Socket Layer, number of iframes and redirects, percentage of white spaces in HTML content
URL based features	Number of deceptive terms in URL like bank and login, length of URL number of digits, forward slashes, question marks, hyphens, underscores, dots, number of equal signs, subdomains, ampersand, subdomains with two letter, semicolons, presence of subdomain, percentage of digits in hostname
Mobile specific features	Number of API calls to sms, tel, smsto, mmsto, mms, geolocation, number of ipa, number of APK

to extract text from the screenshot. The actual identity of the mobile webpage is obtained from the Second Level Domain (SLD) name. If the second level domain is not present in text obtained from the screenshot, then it is an unsafe page and MobiFish will warn the user else webpage is a safe page.

The authors implemented MobiFish on a Google Nexus 4 smartphone which used android 4.2 Operating System. MobiFish performance was evaluated on 100 phishing URLs and their corresponding legitimate URLs as well as on phishing applications. The experimental results validated that the MobiFish method can effectively fight against the phishing attacks.

6.3.2. *Feature based detection*

Tripathi and Gangwani (2017) proposed a technique to detect malicious mobile webpages. This technique uses both static as well as the dynamic features to determine legitimacy of the webpage. The system uses OCR tool to convert screenshot of the webpage into text. When the user enters the URL, system analyses HTML code, JavaScript content, and checks for cross site scripting. Then it is checked if the second level domain is present in the text obtained by converting the webpage screenshot into text. If the second level domain is present in the text, then the webpage is safe, else warning message is displayed to the user. This technique provides higher accuracy and better classification. The browser extension is build to achieve real time feedback.

6.3.3. *MP-Shield*

Bottazzi et al. (2015) proposed MP-Shield, a framework for detecting phishing attacks on mobile webpages. It is an android application that is implemented on Transmission Control Protocol/ Internet Protocol (TCP/IP) stack as proxy service. Its aim is to inspect IP packets originating from and directed to the mobile applications by extracting HTTP get request from the packet. Virtual private network (VPN) service is used to inspect the packets and watchdog engine is used to check if the URL is blacklisted or not. If URL is blacklisted then a warning is shown to user, else classification engine is used to classify URL as legitimate or suspicious. MP-Shield provides high level of security without causing disturbance to the user.

6.3.4. *kAYO*

Amrutkar et al. (2017) designed and implemented kAYO, a browser extension that differentiates between benign and malicious mobile webpages. It is based on the idea that mobile webpages are different from their corresponding desktop webpages. kAYO uses static features of webpages to identify malicious mobile webpages. They used 44 mobile specific features of webpages and out of these 11 are newly addressed features. These features are derived from URL, JavaScript content, HTML and mobile specific capabilities. The feature set includes 12 URL, 10 JavaScript, 14 HTML and 8 mobile specific features. The list of effective features of mobile webpage are discussed in Table 10.

kAYO browser extension works as follows:

1) The user enters the URL in the extension toolbar.
2) Extension toolbar sends URL over Hyper Text Transfer Protocol Secure (HTTPS) to kAYO's backend server.
3) The URL is crawled by the server, and static features are extracted.
4) The feature set is given to kAYO's trained model, and the model then classifies webpage as phishing or legitimate and decision is sent to user's browser.
5) If URL is benign then the extension will render webpage in the browser automatically, else shows a warning message.

Authors collected over 350,000 benign and malicious mobile webpages and identified new static features from these webpages that can distinguish benign webpages from malicious webpages. This data set is used to train kAYO's model. kAYO gives 90% classification accuracy, 89% true positive rate and 8% false positive rate. kAYO browser extension is designed for Firefox Mobile browser. Technique is fast and reliable. Due to efficient feature set, this technique is able to detect new mobile threats that Google safe browsing and VirusTotal can not detect.

6.3.5. *URL based detection*

Chorghe and Shekokar (2016a) proposed a technique for detecting phishing attacks on android mobile devices. This technique is also capable of identifying Zero-day phishing attacks. It consists of five components – extraction of URL, static analysis of URL, foot-printing of webpage, URL based heuristics, and SVM classifier. Blacklist, static analysis, and machine learning algorithms are used to get precise results. It was implemented on Moto G3 android phones having 6.0.1 Android version and system achieved 92% accuracy.

6.3.6. *Phishing blacklist*

Most of the popular anti-phishing techniques make use of blacklist approach. Blacklist is a list of suspicious IP addresses, URLs, and keywords. It determines if the URL is fraud or not. Fraud URL means it is used by attackers for stealing

user's information. Blacklist needs to be frequently updated as it can only detect phishing URLs and IP addresses listed in it (Sharifi and Siadati, 2008). Blacklist is a valuable source used by anti-phishing toolbars to warn users and deny access to fraud phishing websites. Microsoft has used blacklist based anti-phishing solution with Internet Explorer 7. Blacklisting approach is currently used by Chrome, Google search, and Gmail. Limitation of the blacklist is that it does not detect zero day phishing attacks and can identify only 20% of these attacks. The approach works well as long as the list is regularly updated. This method has high accuracy with a less false positive rate.

6.3.7. *Whitelist*

Whitelist contains list of legitimate URLs, and it is opposite of blacklist. Whitelist proposed by Cao et al. (2008) maintains a list of legitimate LUIs and confirms the legitimacy of trustworthy pages that are already present in the whitelist. It prevents users from giving credentials to unrecognised or unauthorised websites. When the user enters their credentials in the trusted LUIs present in whitelist, system will not show any warning. But if there is an attempt to submit sensitive data to LUI that are not in the whitelist, then user's browsing will be stopped and user will be warned about the forgery (Li et al., 2012). Maintaining a whitelist is easy as compared to blacklist because legitimate website hardly change their URLs (Jain and Gupta, 2016). Using the similar concept, Han et al. (2007) proposed an anti-phishing method for smartphone devices. The main concern is that user is not able to differentiate fake LUI from genuine LUI. So, Han et al. proposed a method in which smart devices store the feature information of LUI in advance. Before the user enters authentication information (Jain and Gupta, 2017b) in LUI, a browser plug-in verifies the LUI based on pre-stored LUI information. If LUI passes the verification of smart device, then the device allows to fill the user id and password field. This method significantly improves the security of Login information.

6.4. *Malicious mobile applications detection*

Phishing attack via mobile applications is another major problem faced by mobile device users. Once the malicious application enters the device, it controls device of the user and collects personal information and sends it to the attacker. When applications are installed, they request for many irrelevant permissions that have nothing to do with the working of application. Various approaches to detect malicious applications and methodologies to prevent data leakage from the mobile applications are discussed below.

6.4.1. *VeriUI*

Liu and Cox (2014) proposed a system "VeriUI" based on attested login, which is a password protection mechanism for mobile devices. It provides a secure and hardware isolated surroundings to input password so as to prevent phishing attacks that occur through mobile applications. When the user logs in through VeriUI device, this scheme supplements credentials with software and hardware information of a device and some contextual meta-data. VerUI assures that credentials handling is separated from the rest of application and are processed in a secure environment.

6.4.2. *StopBankun*

There are some malicious applications that aim to steal user's credentials and attack existing mobile applications by replacing them with the modified applications. Kim et al. (2015) proposed a method StopBankun to prevent replacement of banking applications with the malicious applications. Whenever a third party application attempts to remove a legitimate application, PackageInstaller is launched that shows very limited information due to which unaware users allow it to perform actions and the application is removed from the device. The objective of StopBankun is to make PackageInstaller show sufficient information so that the user is able to notice any illegal attempt. Process of removing an application from mobile phone is shown in Fig. 13.

6.4.3. *Confidential data leakage prevention*

Smartphones store huge amount of personal information, such as messages, contacts, etc. and this information is very sensitive. Malicious applications try to access this information via permissions. Canbay et al. (2017) proposed a system for Android devices to prevent confidential data leakage. It uses J48 classification algorithm to detect applications that leak sensitive information. K-Means clustering algorithm is used to evaluate mobile applications downloaded from Google Play Store to check if they have any resemblance to the malicious mobile applications. The system effectively detects malicious and benign applications with 98.6% accuracy.

6.4.4. *SMARTGEN*

URL plays an important role in the detection of phishing attacks but URLs are hidden in mobile applications, unlike desktops where URLs are directly visible. So a mechanism is required with which we can see the URLs in mobile applications. Zuo and Lin (2017) developed a tool SMARTGEN that automatically sends a request message to the server and retrieves the URL for the mobile application. This URL is then submitted to

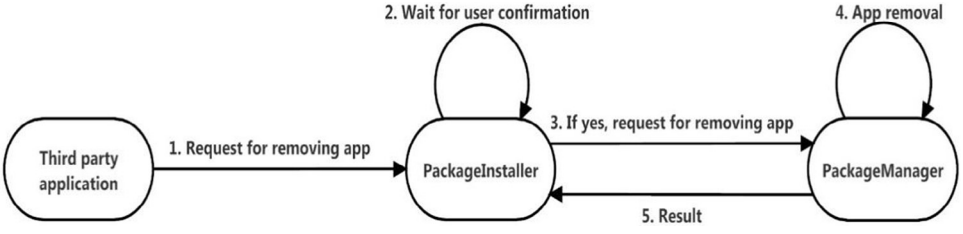

Fig. 13 – Application removal procedure.

a service named "VirusTotal" that detects harmful URLs for security analysis.

6.4.5. *Andromaly*

Shabtai et al. (2012) proposed a light-weight approach for detecting host based malware. The technique observes various features and events of the mobile device and uses machine learning detectors to classify data collected as phishing or legitimate. The results have shown that the proposed technique is effective in detecting malicious software on mobile devices. With the help of Andromaly, suspicious behaviour of an application can be reported to the Android market.

6.4.6. *AppsPlayground*

Rastogi et al. (2013) proposed a framework AppsPlayground for detecting malicious functioning and privacy leakage from the Android applications. AppsPlayground incorporates many components for detection of malicious applications. A wide range of detection techniques are used like Taint Droid, kernel level system monitoring. AppsPlayground analyses for both malware as well as Grayware. This tool effectively evaluates android applications at large scale.

6.4.7. *TrueWalletM*

In order to protect login credentials that are used to access online services over the mobile devices, Bugiel et al. (2010) proposed a secure wallet based system "TruWalletM". This approach uses Trusted Execution Environment (TrEE) and hardware security features present in mobile phones. The method works well with legacy software and standard authentication methods without imposing any performance overhead. Communication process is slightly slowed down. The authors have addressed the issue of run time compromise of interface which results into credentials disclosure. It is a password manager and authentication agent which protects login credentials without requiring the user to trust the operating system.

6.4.8. *RiskRanker*

Grace et al. (2012) proposed a proactive approach to detect zero-day android malware. This approach analyse android applications according to some set of rules that are specifically designed to detect the malicious behaviour of the application and this behaviour is called as potential risks associated with untrusted applications. The risk is divided into three categories – high-risk, medium risk, and low risk. RiskRanker after analysing dangerous behaviour, generates a prioritised list of applications which can be further examined.

6.5. *Quick Response (QR) code based techniques*

QR-code is a two-factor authentication scheme secure under untrusted local systems and servers. It is used to trace the products and store massive data about them. QR code (Liu et al., 2008) is used in many industries, such as an advertisement, sale wrapping, and business cards.

6.5.1. *Single Sign-On based on QR-code*

Mukhopadhyay and Argles (2011) proposed a secure Single Sign-On method that uses mobile QR-code based one time password scheme. Single Sign-On allows a user to login once and access multiple services. Single Sign-On method do not protect users from real-time attacks but in the proposed scheme, the authors gave an anti-phishing Single Sign-On solution which is effective against phishing attacks.

6.5.2. *Authentication scheme using QR-code*

To protect the personal information from phishing attacks on mobile devices Choi et al. (2011) proposed a Single Sign-On authentication scheme based on QR-code. This scheme has addressed the limitation of SingleSign-On which allows the user to access multiple applications with single username and password. In the proposed approach, server generates a random key which is used for secure communication. This scheme works in three phases. First is login request phase, second is QR-code generation phase, and third is verification phase. The scheme encrypts the information due to which attacker can not obtain the information even if the information is exposed to them.

6.6. *Personalized security indicators*

Personalized security indicators are the visual indicators shared between the user and the application. With the help of these indicators, users can identify genuine applications even if malicious applications are present. When the user starts an application for the first time, he is asked to choose an indicator for each application. After that, whenever an application starts, it authenticates itself by showing the indicator which if correct assures the user that it is the legitimate application and user input his credentials and Marforio et al. (2015, 2016a, 2016b) proposed a scheme using personalised security indicators for detection of phishing attacks on mobile applications. With the help of these security indicators, a user can distinguish genuine applications from malicious applications. Various online services are also using personalised security indicators.

7. Open issues and challenges

Many solutions have been given by the researchers to detect and prevent mobile phishing attacks but still, there is no single solution that can detect or prevent all the attacks. Whenever researchers come up with any idea to fight against phishing attacks, attackers change their attacking strategy and find the weaknesses in the current solution. In this section, we have discussed some open challenges that are needed to be addressed.

7.1. *Zero-day phishing attacks*

Foremost issue is to detect and prevent Zero-day phishing attacks. Zero-day attacks are those attacks that take advantage of vulnerabilities on the same day they are made public or in other terms that take advantage of publically known unpatched vulnerabilities. If good guys find these vulnerabilities, they warn the vendor to patch the vulnerability but if attackers find these vulnerabilities, they exploit these vulnerabilities. Zero-day attack may result into installation of malware,

spyware, or unwanted access to user's personal information (BullGuard, 2017). Generally, anti-phishing techniques use blacklisting and whitelisting approaches that are not able to deal with Zero-day phishing attacks and can detect only 20% of them. Currently, there is no solution available that can detect Zero-day phishing attacks with high accuracy.

7.2. *Update requirements of list based approaches*

List based approaches (i.e. Blacklist and Whitelist) need to be updated frequently. These techniques work as long as the user updates the list. These techniques have low false positive rate but at the cost of user verification. Time and efforts required to update these lists reduce their effectiveness.

7.3. *Determining appropriate threshold values*

Threshold is the level of similarity between two instances. Phishing sites look similar to their corresponding legitimate sites. Therefore, level of similarity between the two instances is calculated and compared with threshold value. So, to determine the appropriate threshold value is an important issue in order to get correct results. If the threshold value is greater than the appropriate value, then the false negative rate increases and if the threshold value is smaller than the appropriate value, then the false positive rate increases. A good anti-phishing solution is one having false positive and false negative rate as minimum as possible (Jain and Gupta, 2017a).

7.4. *Language dependencies*

Language dependency is another issue. Different text languages are used over the Internet in websites, and mobile applications. There are some techniques, such as heuristics techniques that are language dependent as they use keywords and feature set. So language dependent techniques fail to work in the situations where a different language is used (Jain and Gupta, 2017a).

7.5. *Selection of appropriate classifier*

Selection of appropriate classifier in machine learning based defending approaches is a challenging task. The good classifier takes minimum training time and gives high detection accuracy. For example, Support vector machine (SVM) is used to classify an instance as phishing or legitimate. But the problem with SVM is that it works for small datasets only. The naïve Bayesian classifier is another popular classifier, but it can be used only when the values of the various features are mutually independent (Amrutkar et al., 2017).

7.6. *Lack of awareness among users*

User awareness about phishing attacks is also an important issue (Parsons et al., 2014). Most of the non-technical users do not want to learn, and out of those who learn, most of them do not retain their knowledge for a long time. Some improvements should be made in the user interface. Active warnings should be given instead of passive warnings.

7.7. *High computation requirement in machine learning*

Currently, machine learning techniques are widely used to detect phishing attack in desktops as well as mobile phones, but these techniques require high computation power to extract features and to process them in real time. So these techniques need to be improved.

8. Conclusion

The aim of phishing attack is to steal user's personal information. Although phishing attack has been targeting the desktop users from a very long time, but now the attackers have shifted their focus to mobile device users. When it comes to mobile phones, the attackers have numerous ways to reach the user and some of them include SMS, mobile applications, e-mails, mobile web browsers, and MMS. Due to small screen size, inconvenience of user input, lack of awareness, mobile device users are three times more vulnerable to phishing attacks as compared to desktop users. Mobile webpages are different from their desktop counterparts in terms of content, layout, and functionality; so separate techniques are needed to avoid these attacks on mobile devices.

Social engineering is one of the most widely used methods to acquire user's information using fake websites, emails, or SMSes. Fraud messages are sent to victims asking them to update their details. Malicious software is installed in user's device either by sending the malicious links or making it available on the application store. It is difficult for the users to ignore SMS they receive on their mobile devices.

User education or training is necessary for creating awareness among the users so that their susceptibility to fall victim to phishing attack can be reduced. Various mobile games have been developed to educate the users about phishing attacks but education alone can not guarantee positive behaviour reaction. Education is necessary but not sufficient in avoiding phishing attacks. User education along with software solutions is required. This paper provides an overview of mobile phishing attacks and various anti-phishing solutions available. Taxonomy of phishing defence mechanism will help users to have an understanding of the topic. There is a broad scope of research that can be done to develop new defence mechanisms to fight against mobile phishing attack, specifically considering the variation of devices.

REFERENCES

Abu-Nimeh S, Nair S. Bypassing security toolbars and phishing filters via DNS poisoning. In Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE (pp. 1–6). IEEE; 2008, November.

Adewole KS, Anuar NB, Kamsin A, Sangaiah AK. SMSAD: a framework for spam message and spam account detection. Multimedia Tools Appl 2017;1–36.

Advantis. Beware of phishing scams in social media; 2017. Available from https://www.advantiscu.org/fraud-prevention/beware-of-phishing-scams-in-social-media.html. [Accessed July 2017].

Almeida TA, Silva TP, Santos I, Hidalgo JMG. Text normalization and semantic indexing to enhance Instant Messaging and SMS spam filtering. Knowledge-Based Syst 2016;108:25–32.
Almomani A, Gupta BB, Atawneh S, Meulenberg A, Almomani E. A survey of phishing email filtering techniques. IEEE Commun Surveys Tutor 2013;15(4):2070–90.
Amrutkar C, Kim YS, Traynor P. Detecting mobile malicious webpages in real time. IEEE Trans Mobile Comput 2017;16(8):2184–97.
Anti-Phishing Working Group (APWG). Phishing activity trends report – first quarter 2016. 2016a. Available from http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf. [Accessed June 2017].
Anti-Phishing Working Group (APWG). Phishing activity trends report – second quarter 2016. 2016b. Available from http://docs.apwg.org/reports/apwg_trends_report_q2_2016.pdf. [Accessed June 2017].
Anti-Phishing Working Group (APWG). Phishing activity trends report – third quarter 2016. 2016c. Available from http://docs.apwg.org/reports/apwg_trends_report_q3_2016.pdf. [Accessed June 2017].
Anti-Phishing Working Group (APWG). Phishing activity trends report – fourth quarter 2016. 2016d. Available from http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf. [Accessed June 2017].
Arachchilage NAG, Cole M. Design a mobile game for home computer users to prevent from "phishing attacks". In Information Society (i-Society), 2011 International Conference on (pp. 485–489). IEEE; 2011, June.
Arachchilage NAG, Cole M. Designing a mobile game for home computer users to protect against phishing attacks. arXiv preprint arXiv:1602.03929; 2016.
Arachchilage NAG, Hameed MA. Integrating self-efficacy into a gamified approach to thwart phishing attacks. arXiv preprint arXiv:1706.07748; 2017.
Arachchilage NAG, Love S. A game design framework for avoiding phishing attacks. Comput Human Behav 2013;29(3):706–14.
Arachchilage NAG, Tarhini A, Love S. Designing a mobile game to thwarts malicious IT threats: a phishing threat avoidance perspective. arXiv preprint arXiv:1511.07093; 2015.
Asanka N, Love S, Scott M. Designing a mobile game to teach conceptual knowledge of avoiding'phishing attacks'. Int J e-Learn Sec 2012;2(1):127–32.
AUJAS. Information Risk management blog, mobile phishing: theif right in your pocket; 2015. Available from https://blog.aujas.com/2015/08/27/mobile-phishing-thief-right-in-your-pockets/. [Accessed July 2017].
Bicakci K, Unal D, Ascioglu N, Adalier O. Mobile authentication secure against man-in-the-middle attacks. Proc Comp Sci 2014;34:323–9.
Bottazzi G, Casalicchio E, Cingolani D, Marturana F, Piu M. MP-Shield: a framework for phishing detection in mobile devices. In: IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), pp. 1977–1983. IEEE; 2015.
Bugiel S, Dmitrienko A, Kostiainen K, Sadeghi AR, Winandy M. TruWalletM: secure web authentication on mobile platforms. In: International conference on trusted systems. Berlin, Heidelberg: Springer; 2010. p. 219–36.
BullGuard. What are zero-day attacks?; 2017. Available from http://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/what-are-zero-day-attacks.aspx. [Accessed July 2017].
Canbay Y, Ulker M, Sagiroglu S. Detection of mobile applications leaking sensitive data. In Digital Forensic and Security (ISDFS), 2017 5th International Symposium on (pp. 1–5). IEEE; 2017, April.
Cao Y, Han W, Le Y. Anti-phishing based on automated individual white-list. In Proceedings of the 4th ACM workshop on Digital identity management (pp. 51–60). ACM; 2008, October.
CAPEC. CAPEC-164: mobile phishing; 2017. Available from https://capec.mitre.org/data/definitions/164.html. [Accessed June 2017].
Carroll A, Heiser G. An analysis of power consumption in a smartphone; 2010.
Choi K, Lee C, Jeon W, Lee K, Won D. A mobile based anti-phishing authentication scheme using QR code. In Mobile IT Convergence (ICMIC), 2011 International Conference on (pp. 109–113). IEEE; 2011, September.
Chorghe SP, Shekokar N. A solution to detect phishing in android devices. In: Information systems security. Springer International Publishing; 2016a. p. 461–70.
Chorghe SP, Shekokar N. A survey on anti-phishing techniques in mobile phones. In Inventive Computation Technologies (ICICT), International Conference on (Vol. 2, pp. 1–5). IEEE; 2016b, August.
Choudhary N, Jain AK. Comparative analysis of mobile phishing detection and prevention approaches. In International conference on information and communication technology for intelligent systems (pp. 349–356). Springer, Cham; 2017a, March.
Choudhary N, Jain AK. Towards filtering of SMS spam messages using machine learning based technique. In: Advanced informatics for computing research. Singapore: Springer; 2017b. p. 18–30.
CISCO. IronPort Now Part of Cisco. Available from https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/ironport.html. [Accessed July 2017].
Cormack GV, Programming Languages Group. 2005 TREC public spam corpus; 2017. Available from https://plg.uwaterloo.ca/~gvcormac/treccorpus/. [Accessed June 2017].
Cranor LF, Egelman S, Hong JI, Zhang Y. "Phinding phish: evaluating anti-phishing tools" In Proceedings of The 14th Annual Network and Distributed System Security Symposium (NDSS '07), February, 2007.
CSMINING Group. Spam Email Dataset; 2010. Available from http://csmining.org/index.php/spam-email-datasets-.html. [Accessed July 2017].
Delac G, Silic M, Krolo J. Emerging security threats for mobile platforms. In MIPRO, 2011 Proceedings of the 34th International Convention (pp. 1468–1473). IEEE; 2011, May.
Delany SJ, Buckley M, Greene D. SMS spam filtering: methods and data. Expert Syst App 2012;39(10):9899–908.
Department of Telematics. SMS spam collection v.1; 2011. Available from http://www.dt.fee.unicamp.br/~tiago/smsspamcollection/. [Accessed June 2017].
Digital Guardian. What is whaling attack, defining and identifying whaling attacks; 2017. Available from https://digitalguardian.com/blog/what-whaling-attack-defining-and-identifying-whaling-attacks. [Accessed July 2017].
Dublin Institute of Technology. DIT SMS spam dataset; 2012. Available from http://www.dit.ie/computing/research/resources/smsdata/. [Accessed June 2017].
Dunham K. *Mobile malware attacks and defense*. Syngress; 2008.
El-Alfy ESM, AlHasan AA. Spam filtering framework for multimodal mobile communication based on dendritic cell algorithm. Fut Gen Comp Syst 2016;64:98–107.
Enron Email Dataset; 2015. Available from https://www.cs.cmu.edu/~./enron/. [Accessed June 2017].
Felt AP, Finifter M, Chin E, Hanna S, Wagner D. A survey of mobile malware in the wild. In Proceedings of the 1st ACM

workshop on Security and privacy in smartphones and mobile devices (pp. 3–14). ACM; 2011, October.
FireEye. Best Defense against Spear Phishing; 2017. Available from https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html. [Accessed July 2017].
Foozy CFM, Ahmad R, Abdollah MF. Phishing detection taxonomy for mobile device. Int J Comp Sci Issues 2013;10(1):338–44.
Gomez Hidalgo, JM. 2011. SMS Spam Corpus v.0.1. Available from http://www.esp.uem.es/jmgomez/smsspamcorpus/. [Accessed July 2017].
Grace M, Zhou Y, Zhang Q, Zou S, Jiang X. Riskranker: scalable and accurate zero-day android malware detection. In Proceedings of the 10th international conference on Mobile systems, applications, and services (pp. 281–294). ACM; 2012, June.
Gupta BB, Arachchilage NA, Psannis KE. Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommun Syst 2017;1–21.
Gupta BB, Tewari A, Jain AK, Agrawal DP. Fighting against phishing attacks: state of the art and future challenges. Neural Comput Appl 2017;28(12):3629–54.
Han W, Wang Y, Cao Y, Zhou J, Wang L. Anti-phishing by smart mobile device. In Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference on (pp. 295–302). IEEE; 2007, September.
Hauri, Smishing defender; 2016. Available from http://www.hauri.co.kr/support/hauriNews_view.html?intSeq=303&page=7&keyfield=&key. [Accessed July 2017].
He D, Chan S, Guizani M. Mobile application security: malware threats and defenses. IEEE Wire Commun 2015;22(1):138–44.
Hong J. The state of phishing attacks. Commun ACM 2012;55(1):74–81.
How-To Geek. What is DNS poisoning; 2016. Available from https://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/. [Accessed July 2017].
IMPERVA. Cross site scripting attacks; 2017. Available from https://www.incapsula.com/web-application-security/cross-site-scripting-xss-attacks.html. [Accessed June 2017].
Infosec institute. Infosec institute session hijacking cheat sheet; 2015. Available from http://resources.infosecinstitute.com/session-hijacking-cheat-sheet/. [Accessed July 2017].
Infosec institute. Phishing on Social Networks – Gathering information; 2017. Available from http://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-attacks-by-demographic/social-networks/#gref.[Accessed July 2017].
Infosec Institute. What is Vishing; 2017. Available from http://resources.infosecinstitute.com/category/enterprise/phishing/phishing-variations/phishing-variations-vishing/what-is-vishing/#gref. [Accessed July 2017].
Jain AK, Gupta BB. A novel approach to protect against phishing attacks at client side using auto-updated white-list. EURASIP J Info Sec 2016;2016(1):9.
Jain AK, Gupta BB. Phishing detection: analysis of visual similarity based approaches. Security and Communication Networks, 2017; 2017a.
Jain AK, Gupta BB. Two-level authentication approach to protect from phishing attacks in real time. J Ambient Intell Humaniz Comput 2017b;1–14.
Jeon W, Kim J, Lee Y, Won D. A practical analysis of smartphone security. Human Interface and the Management of Information. Interacting with Information, 311–320; 2011.
Joo JW, Moon SY, Singh S, Park JH. S-Detector: an enhanced security model for detecting Smishing attack for mobile computing. Telecommun Syst 2017;1–10.
Karami A, Zhou L. Improving static SMS spam detection by using new content-based features; 2014.
Kessem L. Rogue mobile apps, phishing, malware and fraud; 2012. Available from https://blogs.rsa.com/rogue-mobile-apps-phishing-malware-and-fraud. [Accessed July 2017].
Khonji M, Iraqi Y, Jones A. Phishing detection: a literature survey. IEEE Commun Surveys Tutor 2013;15(4):2091–121.
Khurana P, Sharma A, Singh PK. A systematic analysis on mobile application software vulnerabilities: issues and challenges. Ind J Sci Technol 2016;9(32).
Kim D, Park C, Ryou J. StopBankun: Countermeasure of app replacement attack on Android. In Ubiquitous and Future Networks (ICUFN), 2015 Seventh International Conference on (pp. 603–605). IEEE; 2015, July.
Krombholz K, Hobel H, Huber M, Weippl E. Advanced social engineering attacks. J Info Sec Appl 2015;22:113–22.
Landman M. Managing smart phone security risks. In 2010 Information Security Curriculum Development Conference (pp. 145–155). ACM; 2010, October.
Lee A, Kim K, Lee H, Jun M. A study on realtime detecting smishing on cloud computing environments. In: Advanced multimedia and ubiquitous engineering. Berlin, Heidelberg: Springer; 2016. p. 495–501.
Li L, Helenius M, Berki E. A usability test of whitelist and blacklist-based anti-phishing application. In Proceeding of the 16th International Academic MindTrek Conference (pp. 195–202). ACM; 2012, October.
Lifewire. VoIP phishing – what is VoIP phishing and how does it work; 2016. Available from https://www.lifewire.com/voip-phishing-3426534. [Accessed July 2017].
Liu D, Cox LP. Veriui: attested login for mobile devices. In Proceedings of the 15th Workshop on Mobile Computing Systems and Applications (p. 7). ACM; 2014, February.
Liu Y, Yang J, Liu M. Recognition of QR Code with mobile phones. In Control and Decision Conference, 2008. CCDC 2008. Chinese(pp. 203–206). IEEE; 2008, July.
Marforio C, Masti RJ, Soriente C, Kostiainen K, Capkun S. Personalized security indicators to detect application phishing attacks in mobile platforms. arXiv preprint arXiv:1502.06824; 2015.
Marforio C, JayaramMasti R, Soriente C, Kostiainen K, Čapkun S. Evaluation of personalized security indicators as an anti-phishing mechanism for smartphone applications. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 540–551). ACM; 2016a, May.
Marforio C, Masti RJ, Soriente C, Kostiainen K, Capkun S. Hardened setup of personalized security indicators to counter phishing attacks in mobile banking. In Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices (pp. 83–92). ACM; 2016b, October.
Mimecast. Whaling attack; 2017. Available from https://www.mimecast.com/content/whaling-attack/. [Accessed July 2017].
Mobile Ecosystem Forum. MEF mobile messaging fraud report 2016; 2017. Available from https://mobileecosystemforum.com//wp-content/uploads/2016/09/Fraud_Report_2016.pdf. [Accessed June 2017].
Moore T, Clayton R, Stern H. Temporal Correlations between Spam and Phishing Websites. In LEET; 2009, April.
Mukhopadhyay S, Argles D. An Anti-Phishing mechanism for single sign-on based on QR-code. In Information Society (i-Society), 2011 International Conference on (pp. 505–508). IEEE; 2011, June.
Nortan. What is rootkit virus?; 2017. Available from http://www.pctools.com/security-news/what-is-a-rootkit-virus/. [Accessed July 2017].

OpenPhish. Phishing URL. Available from https://openphish.com/feed.txt. [Accessed July 2017].
Ott M. Deceptive onion spam corpus v1.4. Available from http://myleott.com/op_spam/. [Accessed July 2017].
Ott M, Choi Y, Cardie C, Hancock JT. Finding deceptive opinion spam by any stretch of the imagination. In Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies-Volume 1 (pp. 309–319). Association for Computational Linguistics; 2011, June.
Ott M, Cardie C, Hancock JT. Negative deceptive opinion spam. In HLT-NAACL (pp. 497–501); 2013, June.
Parker F, Ophoff J, Van Belle JP, Karia R. Security awareness and adoption of security controls by smartphone users. In Information Security and Cyber Forensics (InfoSec), 2015 Second International Conference on(pp. 99–104). IEEE; 2015, November.
Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Comp Sec 2014;42:165–76.
PCWorld. Types of Phishing Attacks; 2017. Available from http://www.pcworld.com/article/135293/article.html. [Accessed July 2017].
PHISHING.org. History of Phishing. Available from http://www.phishing.org/history-of-phishing. [Accessed July 2017].
Phishingpro. 2017. Available from http://www.phishingpro.com/. [Accessed July 2017].
Phishload. The Phishload phishing test database; 2012. Available from http://www.medien.ifi.lmu.de/team/max.maurer/files/phishload/. [Accessed July 2017].
Phishtank. Join the fight against phishing. Available from https://www.phishtank.com/. [Accessed July 2017].
PHISHING.org. phishing techniques. Available from http://www.phishing.org/phishing-techniques. [Accessed July 2017].
Proofpoint. The Human Factor Report; 2017. Available from https://proofpoint.com/us. [Accessed June 2017].
Rastogi V, Chen Y, Enck W. AppsPlayground: automatic security analysis of smartphone applications. In: Proceedings of the third ACM conference on data and application security and privacy (p. 209–220). ACM. 2013, February.
Richardson R, North M. Ransomware: evolution, mitigation and prevention. Int Manage Rev 2017;13(1):10.
SANS. SANS exploits at the end: SANS 2016 threat landscape survey. Available from https://www.sans.org/reading-room/whitepapers/analyst/exploits-endpoint-2016-threat-landscape-survey-37157. [Accessed July 2017].
Search security. Malware (malicious software); 2016. Available from http://searchsecurity.techtarget.com/definition/malware. [Accessed June 2017].
Search security. Spear phishing; 2017. Available from http://searchsecurity.techtarget.com/definition/spear-phishing. [Accessed July 2017].
Security through education. The Social Engineering Framework; 2017. Available from https://www.social-engineer.org/framework/attack-vectors/smishing/. [Accessed July 2017].
Shabtai A, Kanonov U, Elovici Y, Glezer C, Weiss Y. Andromaly": a behavioral malware detection framework for android devices. J Intell Info Syst 2012;38(1):161–90.
Shahriar H, Zulkernine M. PhishTester: automatic testing of phishing attacks. In Secure Software Integration and Reliability Improvement (SSIRI), 2010 Fourth International Conference on (pp. 198–207). IEEE; 2010, June.
Sharifi M, Siadati SH. A phishing sites blacklist generator. In Computer Systems and Applications, 2008. AICCSA 2008. IEEE/ACS International Conference on (pp. 840–843). IEEE; 2008, March.
Silva RM, Almeida TA, Yamakami A. MDLText: an efficient and lightweight text classifier. Knowledge-Based Syst 2017;118:152–64.
Singh HP, Singh S, Singh J, Khan SA. VoIP: state of art for global connectivity – a critical review. J Netw Comp Appl 2014;37:365–79.
Statista. Number of Smartphone users worldwide from 2014 to 2020; 2017a. Available from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. [Accessed July 2017].
Statista. Worldwide A2P SMS Markets 2014–2017; 2017b. Available from https://www.statista.com/statistics/485153/a2p-sms-market-size-worldwide/. [Accessed September 2017].
Symantec. Symantec internet security threat report 2014, Vol. 19; 2017a. Available from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf. [Accessed July 2017].
Symantec. Symantec security response The Risks of Social Networking; 2017b. Available from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf. [Accessed June 2017].
Tagg C. A corpus linguistics study of SMS text messaging [Doctoral dissertation]. University of Birmingham; 2009.
Tewari A, Jain AK, Gupta BB. Recent survey of various defense mechanisms against phishing attacks. J Info Privacy Sec 2016;12(1):3–13.
The Honeynet Project. Phishing Technique One – Phishing through Compromised Web Servers; 2008. Available from https://www.honeynet.org/node/90. [Accessed July 2017].
Tripathi SJ, Gangwani VS. Design the framework for detecting malicious mobile webpages in real time. Int J Eng Sci 2017;11884.
Uysal AK, Gunal S, Ergin S, Gunal ES. A novel framework for SMS spam filtering. In Innovations in Intelligent Systems and Applications (INISTA), 2012 International Symposium on (pp. 1–4). IEEE; 2012, July.
Wandera. Wandera Mobile data report: focus on Phishing; July 2017. Available from http://go.wandera.com/rs/988-EGM-040/images/Phishing%20%282%29.pdf. [Accessed June 2017].
Wu L, Du X, Wu J. MobiFish: a lightweight anti-phishing scheme for mobile phones. In Computer Communication and Networks (ICCCN), 2014 23rd International Conference on (pp. 1–8). IEEE; 2014, August.
Wu L, Du X, Wu J. Effective defense schemes for phishing attacks on mobile computing platforms. IEEE Trans Vehicular Technol 2016;65(8):6678–91.
Yadav K, Kumaraguru P, Goyal A, Gupta A, Naik V. Smsassassin: crowdsourcing driven mobile-based system for sms spam filtering. In Proceedings of the 12th workshop on mobile computing systems and applications (pp. 1–6). ACM; 2011, March.
Yang W, Xiong A, Chen J, Proctor RW, Li N. Use of phishing training to improve security warning compliance: evidence from a field experiment. In Proceedings of the hot topics in science of security: symposium and bootcamp (pp. 52–61). ACM; 2017, April.
Yeboah-Boateng EO, Amanor PM. Phishing, SMiShing& Vishing: an assessment of threats against mobile devices. J Emerg Trends Comput Info Sci 2014;5(4):297–307.
Zuo C, Lin Z. SMARTGEN: exposing server URLs of mobile apps with selective symbolic execution. In Proceedings of the 26th International Conference on World Wide Web (pp. 867–876). International World Wide Web Conferences Steering Committee; 2017, April.

Diksha Goel has received her B.Tech. degree in Computer Science and Engineering from UIET, Kurukshetra, India. Currently, she is pursuing M.Tech. in Computer Engineering (Specialization in Cyber Security) from National Institute of Technology, Kurukshetra, Haryana, India. Her research interest includes Mobile security, Web security, Machine learning and Smishing detection.

Ankit Kumar Jain is presently working as Assistant Professor in National Institute of Technology, Kurukshetra, India. He received Master of technology from Indian Institute of Information Technology Allahabad (IIIT) India. Currently, he is pursuing PhD in cyber security from National Institute of Technology, Kurukshetra. His general research interest is in the area of Information and Cyber security, Phishing Website Detection, Web security, Mobile Security, Online Social Network and Machine Learning. He has published many papers in reputed journals and conferences.