Praise Worthy Prize

International Review on Computers and Software (I.RE.CO.S.), Vol. 9, N. 10
ISSN 1828-6003 *October 2014*

A Practical Rule Based Technique by Splitting SMS Phishing from SMS Spam for Better Accuracy in Mobile Device

Cik Feresa Mohd Foozy, Rabiah Ahmad, Faizal M. A.

Abstract – *Short Message Service (SMS) is one of the popular communication services. However, this can contribute to increasing mobile device attacks. Presently, SMS phishing (SMiShing) attack is alarming to the mobile phone users because these attacks usually succeed in stealing information and money. Moreover, SMS phishing and spam are two different types of attack and level of risk. Thus, it is important to have a SMS phishing corpus. The established SMS corpus is limited to spam and none can be found suitable for SMS Phishing. This study proposes a technique to split the class of SMS phishing from SMS spam and produce better accuracy using the Bayesian technique. The result shows that the enhanced SMS corpus gets 99.8064% accurate classification. The study identified classes and generated an improvement of SMS Phishing corpus which has been labelled in three different classes ie., Ham, Spam and Phishing with better accuracy.*

Keywords: *Classification, Detection, Phishing, Security, SMS, Spam*

I. Introduction

Phishing is one of the various social engineering attacks that is continuously arising on mobile devices recently. Many researches claim that a phishing attack is designed to steal valuable information such as credit card and social security numbers, user IDs and passwords [1], [2]. According to Boodae [2], mobile device users are three times more likely to enter a web-based phishing attack than desktop users. In addition, phishing can attack through browser and email [3]. However, it also can attack via Bluetooth, SMS, Voice Over IP, mobile applications and mobile browsers. It is widely accepted that attack via SMS phishing or SMiShing is increasing [4]-[6]. A smart defence mechanism is highly required to combat this issue. The big challenge however, are that current studies on SMS attack detection are mainly focusing on SMS spam detection and filtering. Up to date, no study has proposed detection technique for SMiShing. As various types of established SMS spam corpus are available publicly over the Internet, a detection model is improved by differentiating phishing class from spam class by its proposed phishing features.

The basic model of splitting and extracting SMS phishing from SMS spam was proposed by Beck [7].

In this study, the extraction of the SMS phishing was done from SMS spam sample. Additionally, Nazario [8] also identified a set of phishing email in his spam email.

He gave an idea to develop email phishing corpus by using Bayesian spam classifier then labelling the spam email as phishing email. This is because there is no public phishing email corpus available for research, therefore a similar yet simple approach was used in this study in detecting the SMS phishing in SMS spam class.

Since a mobile device has a small storage and processor capability, a simple but efficient approach is needed to separate the SMS phishing from SMS spam class.

To separate SMS Phishing from SMS spam, a practical rule is applied based on the technique which contain the features of phishing SMS. The public SMS spam corpus that will be used has been downloaded from UCI Machine Learning and the corpuses are collected from Almeida and Hidalgo [9] and Nazario [10].

This SMS spam corpus only contains two classes of SMS ham and SMS spam. Since SMS phishing attack also has been increasing and affecting the security and privacy of users, there was more motivation to develop SMS phishing corpus which contain SMS ham, spam and phishing for SMS phishing detection study.

The reason the SMS phishing was not self collected is because the data collection process will need extra time and cost. Beck [7] also has proposed a modified Bayesian technique to separate email phishing from email spam.

The difference between the technique of Beck [7] and the proposed technique in this research is that Beck [7] extracts a set of phishing word based on collection of email phishing. Then, run experiment on other email datasets by using the Bayesian technique. Whereas the technique proposed in this research runs the modified SMS datasets that contain ham, spam and phishing class in WEKA tools [11] to get accurate results of the datasets.

In addition, this proposed framework does not include the process of identification and extracting the SMS phishing word. This is because, until this paper was written, there was no SMS phishing available publicly for SMS phishing studies, thus the rule that was applied

on the SMS spam class was to again classify if the SMS will be in spam or in a new phishing class.

Current studies on SMS detection are focusing in detecting SMS spam and not SMS phishing. Several reports has identified that SMS phishing have higher risk than SMS spam and GetSafeOnline [12], a security website identified that not all spam are scam but all phishing are scam. This statement shows the risk level of phishing attack is more serious than spam attack.

Most of the tips in detecting phishing attack suggests to avoid clicking on any strange URL address in the SMS. According to S. Abu-Nimeh, *et al* .[13] and Shah [14], SMS phishing will trick users with a fake URL and by clicking on the URL, a fraudulent website will be launched and the malware will be downloaded onto the mobile device. Moreover, SMS phishing attack has been discussed by Dunham [15] and Salem *et al.* [16].

K. Dunham [15] explained that SMS phishing is a new tactic to spread malware by adding the URL links in SMS and influencing the recipient to click on the URL.

However, not all SMS which contains a URL is phishing. Thus, in this study, the SMS phishing will be separated from SMS spam class and not all URL in SMS spam class should be in the phishing category. Some of the URL is valid and the website exists. Thus, to replace SMS spam that contain URL to the phishing class is not proposed. As an alternative, a rule based technique was developed to split the SMS phishing from SMS spam according to the spam and phishing theory.

Thus, the contribution of this paper is a rule based technique that will separate SMS phishing from SMS spam class and then generate an enhanced SMS phishing corpus. The rest of this paper is as follows: Section 2, is Related Work that will discuss in detail the current study of SMS Scam Detection, SMiShing and SMS Spam Characteristics and the Rule Based Theory. Section 3, is on the Methodology of proposing SMS Phishing Corpus. For section 4, will be the Analysis and Result of the SMS Phishing Corpus and classification experiment that will be run to see the accuracy of the classification using the Bayesian Classification technique. Finally is section 5, with conclusion and further studies.

II. Related Work

There are many tools and software that can be installed in the mobile device to ensure all data are protected and secure from any attacks but the information security problem still arises. According to Leavitt [17], phishing attacks are rapidly growing on mobile devices. Moreover, Joe and Shim [18] said incoming SMS phishing makes the SMS recipient feel their personal privacy is violated. The increasing attack is because mobile phones is one of the important devices to communicate nowadays. F-Secure [19] reported that SMS services usually has a hidden charge on replying SMS phishing. The phishes will not only get money but also information about mobile device versions, contact numbers and others.

Conventionally, SMS phishing will be sent in high volumes but the current trend shows that SMS was sent in small quantities for the purpose of monitoring the security level of the mobile device. In addition, the problem with SMS phishing detection study is the use of SMS language such as "*contact*" will be typed as "*ctct*" or "*contct*". Thus, it will be hard to identify the specific phishing word for SMS phishing compared to other phishing attacks.

II.1. SMS Scam Detection

Generally, SMS architecture contains Sender/Receiver, Protocol, Timestamp and payload (SMS content) behaviour. Each of this behaviour contains a log of the mobile device and the most valuable information are in the SMS payload which contain texts, numbers and symbols in the message where the style of message can be learned and predicted by using machine learning techniques.

J. W. Yoon *et al.* [20] and Peizhou *et al.*[21] studied the SMS content-based with challenge-response scheme where J. W. Yoon *et al.* [20] applied cryptography and CAPCHA and Peizhou *et al.* [21] combined the blacklisting techniques and CAPCHA to detect SMS spam. In addition, Gòmez Hidalgo *et al.* [22] had proposed a content-based SMS spam filtering for dual language of English and Spanish SMS spam using the Bayesian filter technique. Moreover, T. M. Mahmoud and A. M. Mahfouz [23] applied whitelisting techniques to detect content of SMS phishing and Q. Xu *et al.* [24] proposed SMS filtering on non content-based using SVM and KNN techniques.

In addition, Joe and Shim[18] also uses SVM techniques with thesaurus and applied in Windows environment. Several experiments were done by Cormack *et al.* [25] on SMS filtering using 5 types of spam filter tools and similarly, Najadat *et al.* [26], observed several classifier techniques and did a comparison of accuracy to detect spam SMS.

Machine learning technique also has been applied in detecting SMS. Studies that has been done by Xiang *et al.* [27] and Cai *et al.*[28] shows an improvement on the spam filter using traditional balanced Winnow algorithm which is a linear-threshold classification algorithm to detect SMS in Chinese language. Moreover, Wu *et al.* [29] proposed a real time monitoring and filtering SMS system by using Bayesian filtering and Pinyin Fuzzed keyword pattern machine. Jie *et al.* [30] also applied the matching pattern technique. In addition, Uysal [31], also proposed a novel framework using the Bayesian technique but with a dual feature selection technique.

An independent mobile device filtering by Taufiq Nuruzzaman *et al.* [32] using Naïve Bayes technique has been proposed and they proved that spam filtering can be applied independently on the mobile device. Yadav [33]-[34] developed an application called SMSAssassin that uses the Bayesian technique and blacklist words in the system.

T. M. Mahmoud and A. M. Mahfouz [23] applied an artificial immune system technique and the result shows the proposed technique is better than the Naive Bayesian algorithm. Charninda *et al.* [35] proposed a hybrid solution of neural network and Bayesian filtering.

A verification technique has been proposed by Verma *et al.* [36] to add a verifying mechanism in the application.

In the Cryptography area, Saxena [37] has proposed a secure SMS protocol for SMS transmission and a cryptographic algorithm in the SIM card. Moreover, Pereira *et al.* [38] also proposed a lightweight cryptography algorithm to mitigate SMS security issues. In addition, Choi [39] applied the *Common Public Key Cryptography* technique for SMS communication efficiency.

Vall and Rosso [40] did experiments that compared plagiarism detection tools with machine learning detection techniques. Rafique *et al.* [41] applied the Hidden Markov Model (MHH) in SMS protocol for real time detection and compared four evolutionary algorithm and non evolutionary algorithm classification. Que and Farooq [42] also applied MHH on a byte level distribution of SMS. In addition, SMS-Watchdog SMS detection scheme by Yan *et al.*[43] has been developed using anomaly detection methods by identifying the SMS user behaviour in the Windows based.

Until this paper was written, only non technical studies were done by [13], [15], [16] and [44],. However, for SMS phishing technical analysis, this study is the first to separate the SMS phishing from SMS spam corpus.

II.2. SMiShing and SMS Spam Characteristics

Spam not only gives risk to the user, but also affect the organization [45]. In addition, phishing attack also has a high impact on users and organizations. However, in the SMS research area, the study only focuses on detecting SMS spam and not for SMS phishing.

SMS Spam and phishing attacks have different definitions and this was agreed by Toolan and Carthy [46], Mistry *et al.* [47] and S. S. Chandran and S. Murugappan [48]. They defined SMS spam as containing advertisement of marketing.

Additionally, phishing message is a social engineering method that contain messages to trick the user response to the SMS. After that, the malicious web site will display and unfortunately the malware will be downloaded. As a consequence of that, phishes can get information of mobile device, contact number, bank account, track location and others.

From the findings of this study, several characteristic of SMiShing attack has been identified and these characteristic were also implemented to separate SMS phishing from SMS spam. The characteristic of SMS phishing consists of:

- malicious URL [13]-[15], [49]and [44],
- malicious Telephone Number [44],
- asking to unsubscribe the service [49],
- self answering SMS for YES as agree to subscribe [50],
- Announce the SMS recipient as a winner in a contest or competition that was never entered or
- Asking for help to get profit such as need money to eat or reload prepaid phones.

However, SMS spam will contain:

- Marketing campaigns [40], [26], [34], [23], [24], [32], [41], [42] or
- Spread news [24]

The similarity of SMiShing and SMS spam are that both of them are unwanted SMS and the SMS sender's number is not in the SMS recipient's telephone number contact list. However, it is difficult to identify if the telephone number is malicious or not unless the application connects with the contact directory.

For this study, one of the SMS Phishing characteristics above will be the parameter for the decision making of whether the SMS is phishing or spam. The features selection will contain Marketing Advertisements and Winning Announcements. The Methodology section will discuss further how SMS phishing is separated from SMS spam data.

II.3. Rule Based Theory

The rule based approach is a part of an expert system area and several studies have applied this method for decision making. Peizhou, Xiangming *et al.* [21] said the common SMS content-based filtering method are rule-based techniques. The study to detect phishing attacks using the rule based technique has been done by R.B. Basnet *et al.* [51], which generated 15 rule sets that was analyzed using machine learning techniques. Moreover, Shreeram [52] proposed a rule set to detect phishing attacks using genetic algorithms.

Salem [16] have proposed a rule set in the studies for the awareness program and artificial intelligent tools to detect phishing emails. Liping *et al.* [53] had examined seven features for phishing email detection. In addition, Pamunuwa *et al.* [54], proposed to detect phishing email by using IDS.

Alnajim and Munro [55] studied on phishing detection in websites. Zhou *et al.* [56] also proposed to detect phishing attacks and Aburrous *et al.* [57] had listed several criteria to detect phishing and the technique that was applied was the fuzzy technique. SpoofGuard, which has been discussed by Huajun *et al.* [58], is a popular anti-phishing tool. The author also studied several criteria to detect phishing.

There are several tactics to spread phishing email and web sites but there are still less for SMS Phishing and SMS spam. Uniform Resource Locator (URL) is an address of website which is one of the important features to detect phishing attacks. Moreover, URL phishing detection also has been widely applied to detect mobile web phishing and email phishing. Nevertheless, for SMS phishing attacks, detecting phishing through URL is important as one of the features to detect SMS phishing

because this attack will trick users by sending an SMS with malicious URL [13]-[15], [49] and [44].

These solution for mobile web phishing using URL has been studied by Niu [59] and Weili *et al.* [60].

Niu [59] proposed to design an important and short URL to be displayed on safari browser on the iPhone mobile device. Weili *et al.* [60] applied a URL checker in their anti login interface framework. Yadav *et al.* [33] also applied URL features to detect SMS ham and SMS spam but not SMS phishing.

However, since this study only focuses on separating phishing SMS from spam class, not all URLs are malicious. Some URLs contains a valid format or have existing websites.

Thus, new feature selections such as Winning Announcement SMS and Advertisement SMS was applied to improve accuracy result. Moreover, based on the understanding of spam and phishing SMS, these two features differentiate the spam and phishing SMS.

III. Methodology

The aim of this paper is to separate SMS phishing from SMS spam class in SMS spam Corpus that has been downloaded from UCI Machine Learning. The features of SMS phishing are based on the phishing characteristics that has been discussed in the previous section such as fake URLs, winning announcement and free gifts and request to response.

The SMS phishing characteristics were gained from various conference papers and journals from digital library IEEE Xplore, ScienceDirect, ACM Digital Library and SpringerLink. In this study, English SMS spam corpus are based on [61], [62] and [22] datasets that has been downloaded from the UCI Machine Learning [9].

The total SMS that were downloaded were 5572, however after pre-processing data such as redundancy removal, 5166 of SMS spam corpus was applied. There are two classes of ham and spam SMS in this datasets which consist of 4515 SMS ham and 651 SMS spam. Table I, shows the SMS spam specification that has been downloaded.

Fig. 1 below is a generic rule flows how the separating phishing SMS to SMS spam is done.

TABLE I
ENGLISH SMS SPAM SPECIFICATION

English SMS Corpus Specification	English SMS
No of messages	5166
No of words	79748
No of class	2 (Ham and Spam)
Average no of words per message	14.17928
Collection methods and procedures	Download at UCI Machine Learning
Composition of text	Mobile Device user
Language of communication	English
Type of communication	SMS from Unknown Sender, Advertisement, Personal communication

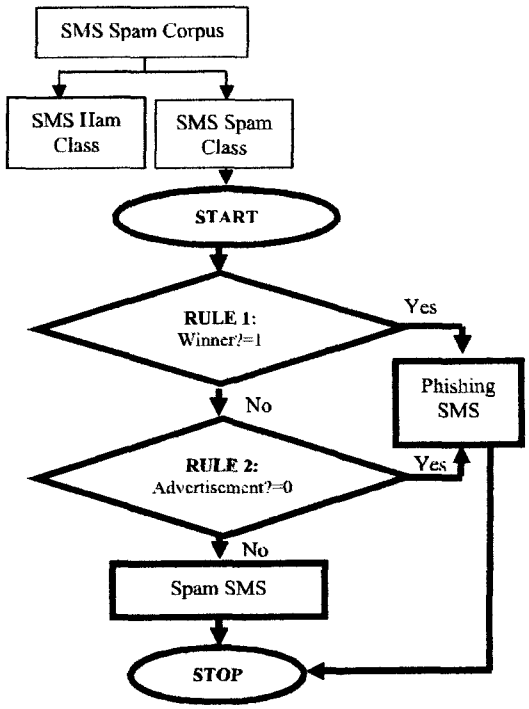

Fig. 1. Generic Process of Rule-Based Decision Making to Separate SMS Phishing from SMS Spam

Step 1: Pre-Processing the entire SMS Spam corpus such as removing SMS redundancy and tokenize

Step 2: Applied four rules to make decision making:

Rule 1: IF the SMS is an winner announcement, THEN result=1

Rule 2: IF the SMS is a marketing advertisement THEN result=1

STEP 1 storing and handling SMS spam corpus using Microsoft Office Excel and pre-processing the SMS to clean the data from noise. STEP 2 is how the rule based performs. There will be no issue of the generated SMS phishing being misconstrued as a ham SMS because the rules are only for SMS spam class from the UCI Machine Learning website.

For Rule 1, the screening words of keyword "*reward*" and "*win*" is a word to initiate user to respond to the SMS. Thus, if the SMS inform the recipient that they won, the result will be 1 as TRUE. For rule 2, if the SMS is an advertisement SMS, it also will be TRUE.

IV. Analysis and Findings

From the analysis that was done on the SMS spam corpus that was downloaded from the UCI Machine Learning, there are several SMS phishing that has been identified on SMS spam. After the pre-processing process, there are 4515 SMS ham and 651 SMS spam and the result after Step 1 until Step 3 was applied, 4512

SMS ham, 567 SMS Spam and 84 SMS spam has been identified (Table II).

Moreover, this SMS phishing corpus has been analysed using the WEKA tool [11] for evaluation of the accuracy classification.

TABLE II
SUMMARY OF SMS SPAM AND ENHANCED SMS PHISHING CORPUS

Dataset	Before Applied Rule-Based			After Applied Rule-Based		
SMS Spam	Ham	Spam	Phishing	Ham	Spam	Phishing
Dataset [9],[10]	4515	651	0	4515	567	84

After SMS Phishing Datasets has been developed using the proposed rule-based technique, an experiment was done using the WEKA tool [11] to validate the proposed rule based technique. True Positive Rate (TPR), False Positive Rate (FPR), False Negative Rate (FNR), and True Negative Rate (TNR) of SMS Phishing Datasets have been identified using the WEKA tool.

To get the result of accuracy level, the SMS phishing features was constructed based on literature review. In addition, there are several Machine Learning techniques in the WEKA tool, however in this paper the Bayesian technique was applied to check the classification of accuracy rate of SMS ham, spam and phishing.

Based on the result in Table III, the accuracy of these SMS Phishing Corpus show high accuracy compared to SMS spam Corpus.

TABLE III
RESULT SMS DETECTION USING BAYESIAN TECHNIQUE

Parameter	Bayesian Technique using WEKA Tool		
	Ham	Phishing	Spam
True Positive	1	1	0.984
False Positive	0.012	0	0
Correctly Classified		99.8064 %	
Incorrectly Classified		0.1936 %	

V. Conclusion

As a conclusion, SMS phishing and spam have different characterizations and security risks. Since there are no available SMS Phishing corpus in the English language, this study is the first to propose a practical rule based technique to separate SMS phishing from SMS spam class.

Two new features are also introduced in this study such as the Winning Announcement SMS and Advertisement SMS. These two features has been added because of the main characteristics of SMS phishing and spam where generally, SMS phishing will contain an winning announcement and SMS spam that will broadcast marketing advertisement.

Additionally, based on the experiments result in Table II, the proposed rule based with these new features has shown the availability to separate the SMS phishing class from SMS spam and generated a SMS phishing corpus for further study in SMS phishing attack which has been increased nowadays. According to the proposed rule based system, the result shows better accuracy for SMS Phishing compared to SMS spam. It is due to the separating process. The result however look only limited to SMS corpus by Almeida and Hidalgo [9] and Nazario [10]. Further study, will be tested using Malay SMS corpus for explore the efficiency of this method.

Acknowledgements

The authors would like to thank Universiti Teknikal Malaysia Melaka (UTeM), Universiti Tun Hussein Onn Malaysia(UTHM) and Ministry of Higher Education Malaysia for supporting this research. This research is funded by MOHE under Long Research Grant Scheme LRGS/2011/FTMK/TK01/1R00002.

References

[1] Microsoft. (2011, 8th June). *Email and web scams: How to help protect yourself.* Available: http://www.microsoft.com/security/online-privacy/phishing-scams.aspx

[2] M. Boodae, "Mobile Users Three Times More Vulnerable to Phishing Attacks," in *Trusteer* vol. 2012, ed, 2011.

[3] P. Soni, *et al.*, "A phishing analysis of web based systems," presented at the Proceedings of the 2011 International Conference on Communication, Computing \&\#38; Security, Rourkela, Odisha, India, 2011.

[4] C. F. M. Foozy, *et al.*, "Phishing Detection Taxonomy for Mobile Device," *International Journal of Computer Science Issues (IJCSI)*, vol. 10, 2013.

[5] A. Kang, *et al.*, "Security Considerations for Smart Phone Smishing Attacks," in *Advanced in Computer Science and its Applications*, ed: Springer, 2014, pp. 467-473.

[6] D. Kim and J. Ryou, "SecureSMS: prevention of SMS interception on Android platform," presented at the Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication, Siem Reap, Cambodia, 2014.

[7] K. Beck and J. Zhan, "Phishing Using a Modified Bayesian Technique," in *Social Computing (SocialCom), 2010 IEEE Second International Conference on*, 2010, pp. 649-655.

[8] J. Nazario, "Phishing Corpus," vol. 2013, ed, 2005.

[9] T. A. Almeida and J. M. G. Hidalgo. (2012, 23 September 2012). *SMS Spam Collection Data Set.* Available: http://archive.ics.uci.edu/ml/datasets/SMS+Spam+Collection

[10] J. Nazario, "Phishing Corpus," 2004-2007.

[11] E. F. Mark Hall, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, Ian H. Witten, "The WEKA Data Mining Software: An Update," *SIGKDD Explorations*, vol. 11, 2009.

[12] GetSafeOnline. (2012, 1 January 2013). *Spam & Scam email.* Available: http://www.getsafeonline.org/protecting-your-computer/spam-and-scam-email/

[13] S. Abu-Nimeh, *et al.*, "Distributed Phishing Detection by Applying Variable Selection Using Bayesian Additive Regression Trees," in *Communications, 2009. ICC '09. IEEE International Conference on*, 2009, pp. 1-5.

[14] J. Shah, "Online crime migrates to mobile phones," *Sage*, vol. 1, pp. 22-23, 2007.

[15] K. Dunham, "Chapter 6 - Phishing, SMishing, and Vishing," in *Mobile Malware Attacks and Defense*, D. Ken, Ed., ed Boston: Syngress, 2009, pp. 125-196.

[16] O. Salem, *et al.*, "Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 2010, pp. 1418-1423.

[17] N. Leavitt, "Mobile Security: Finally a Serious Problem?," *Computer*, vol. 44, pp. 11-14, 2011.

[18] I. Joe and H. Shim, "An SMS Spam Filtering System Using Support Vector Machine," in *Future Generation Information Technology*, vol. 6485, T.-h. Kim, *et al.*, Eds., ed: Springer Berlin

Heidelberg, 2010, pp. 577-584.
[19] F-Secure, "Mobile Threat Report Q3 2012," F-Secure Labs2012.
[20] J. W. Yoon, *et al.*, "Hybrid spam filtering for mobile communication," *Computers & Security*, vol. 29, pp. 446-459, 2010.
[21] H. Peizhou, *et al.*, "A Novel Method for Filtering Group Sending Short Message Spam," in *Convergence and Hybrid Information Technology, 2008. ICHIT '08. International Conference on*, 2008, pp. 60-65.
[22] J. M. G. Hidalgo, *et al.*, "Content based SMS spam filtering," presented at the Proceedings of the 2006 ACM symposium on Document engineering, Amsterdam, The Netherlands, 2006.
[23] T. M. Mahmoud and A. M. Mahfouz, "SMS Spam Filtering Technique Based on Artificial Immune System," *IJCSI International Journal of Computer Science Issues*, vol. 9, 2012.
[24] Q. Xu, *et al.*, "SMS Spam Detection using Content-less Features," *Intelligent Systems, IEEE*, vol. PP, pp. 1-1, 2012.
[25] G. V. Cormack, *et al.*, "Feature engineering for mobile (SMS) spam filtering," presented at the Proceedings of the 30th annual international ACM SIGIR conference on Research and development in information retrieval, Amsterdam, The Netherlands, 2007.
[26] H. Najadat, *et al.*, "Mobile SMS Spam Filtering based on Mixing Classifiers."
[27] Y. Xiang, *et al.*, "Filtering mobile spam by support vector machine " presented at the Conference on Computer Sciences, Software Engineering, Information Technology, E-Business and Applications (3rd: 2004 : Cairo, Egypt), Cairo, Egypt, 2004.
[28] C. Jie, *et al.*, "Spam Filter for Short Messages Using Winnow," in *Advanced Language Processing and Web Information Technology, 2008. ALPIT '08. International Conference on*, 2008, pp. 454-459.
[29] W. Ningning, *et al.*, "Real-time monitoring and filtering system for mobile SMS," in *Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference on*, 2008, pp. 1319-1324.
[30] J. Huang, *et al.*, "A Bayesian Approach for Text Filter on 3G Network," in *Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on*, 2010, pp. 1-5.
[31] A. K. Uysal, *et al.*, "A novel framework for SMS spam filtering," in *Innovations in Intelligent Systems and Applications (INISTA), 2012 International Symposium on*, 2012, pp. 1-4.
[32] M. Taufiq Nuruzzaman, *et al.*, "Simple SMS spam filtering on independent mobile phone," *Security and Communication Networks*, vol. 5, pp. 1209-1220, 2012.
[33] K. Yadav, *et al.*, "SMSAssassin: crowdsourcing driven mobile-based system for SMS spam filtering," presented at the Proceedings of the 12th Workshop on Mobile Computing Systems and Applications, Phoenix, Arizona, 2011.
[34] K. Yadav, *et al.*, "Take Control of Your SMSes: Designing an Usable Spam SMS Filtering System," in *Mobile Data Management (MDM), 2012 IEEE 13th International Conference on*, 2012, pp. 352-355.
[35] T. Charninda, *et al.*, "Content based hybrid sms spam filtering system," 2014.
[36] R. K. Verma, *et al.*, "Extraction and Verification of Mobile Message Integrity," in *Communication Systems and Network Technologies (CSNT), 2011 International Conference on*, 2011, pp. 49-53.
[37] N. Saxena and N. S. Chaudhari, "SecureSMS: A secure SMS protocol for VAS and other applications," *Journal of Systems and Software*, vol. 90, pp. 138-150, 2014.
[38] G. C. C. F. Pereira, *et al.*, "SMSCrypto: A lightweight cryptographic framework for secure SMS transmission," *Journal of Systems and Software*, vol. 86, pp. 698-706, 2013.
[39] J. Choi and H. Kim, "A Novel Approach for SMS security," *International Journal of Security & Its Applications*, vol. 6, 2012.
[40] E. Vall and P. Rosso, "Detection of near-duplicate user generated contents: the SMS spam collection," presented at the Proceedings of the 3rd international workshop on Search and mining user-generated contents, Glasgow, Scotland, UK, 2011.
[41] M. Z. Rafique, *et al.*, "Application of evolutionary algorithms in detecting SMS spam at access layer," presented at the Proceedings of the 13th annual conference on Genetic and evolutionary computation, Dublin, Ireland, 2011.
[42] M. Z. R. que and M. Farooq, "SMS Spam Detection By Operating On Byte-Level Distributions Using Hidden Markov Models (HMMS)," presented at the Virus Bulletin Conference September 2010, 2010.
[43] G. Yan, *et al.*, "SMS-Watchdog: Profiling Social Behaviors of SMS Users for Anomaly Detection Recent Advances in Intrusion Detection," vol. 5758, E. Kirda, *et al.*, Eds., ed: Springer Berlin / Heidelberg, 2009, pp. 202-223.
[44] S. Lee. (2012, *Smishing: SMS + Phishing, Present And On The Rise On Android.* Available: http://www.alertboot.com/blog/blogs/endpoint_security/archive/2012/11/14/smishing-sms-phishing-present-and-on-the-rise-on-android.aspx
[45] Karthika Renuka, D., Visalakshi, P., Blending firefly and bayes classifier for email spam classification, (2013) *International Review on Computers and Software (IRECOS)*, 8 (9), pp. 2168-2177.
[46] F. Toolan and J. Carthy, "Feature selection for Spam and Phishing detection," in *eCrime Researchers Summit (eCrime), 2010*, 2010, pp. 1-12.
[47] N. Mistry, *et al.*, "Preventive Actions to Emerging Threats in Smart Devices Security," 2011.
[48] Chandran, S.S., Murugappan, S., Spam detection and elimination of messages from twitter, (2013) *International Review on Computers and Software (IRECOS)*, 8 (10), pp. 2438-2443.
[49] L. Kriel, *et al.*, "Towards a computer security induction manual for non-IT citizens."
[50] A. Mahajan, *et al.*, "Identification of Fake SMS generated using Android Applications in Android Devices."
[51] R.B. Basnet , *et al.*, "Rule-Based Phishing Attack Detection," *International Conference on Security and Management SAM11 (2011)*, 2011.
[52] V. Shreeram, *et al.*, "Anti-phishing detection of phishing attacks using genetic algorithm," in *Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on*, 2010, pp. 447-450.
[53] M. Liping, *et al.*, "Automatically Generating Classifier for Phishing Email Prediction," in *Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on*, 2009, pp. 779-783.
[54] H. Pamunuwa, *et al.*, "An Intrusion Detection System for Detecting Phishing Attacks," in *Secure Data Management*. vol. 4721, W. Jonker and M. Petkovic, Eds., ed: Springer Berlin / Heidelberg, 2007, pp. 181-192.
[55] A. Alnajim and M. Munro, "An Approach to the Implementation of the Anti-Phishing Tool for Phishing Websites Detection," in *Intelligent Networking and Collaborative Systems, 2009. INCOS '09. International Conference on*, 2009, pp. 105-112.
[56] C. V. Zhou, *et al.*, "A Self-Healing, Self-Protecting Collaborative Intrusion Detection Architecture to Trace-Back Fast-Flux Phishing Domains," in *Network Operations and Management Symposium Workshops, 2008. NOMS Workshops 2008. IEEE*, 2008, pp. 321-327.
[57] M. Aburrous, *et al.*, "Intelligent Phishing Website Detection System using Fuzzy Techniques," in *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*, 2008, pp. 1-6.
[58] H. Huajun, *et al.*, "Countermeasure Techniques for Deceptive Phishing Attack," in *New Trends in Information and Service Science, 2009. NISS '09. International Conference on*, 2009, pp. 636-641.
[59] Y. Niu, *et al.*, "iPhish: Phishing Vulnerabilities on Consumer Electronics," in *UPSEC*, 2008.
[60] H. Weili, *et al.*, "Anti-Phishing by Smart Mobile Device," in *Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference on*, 2007, pp. 295-302.
[61] G. V. Cormack, *et al.*, "Spam filtering for short messages," presented at the Proceedings of the sixteenth ACM conference on Conference on information and knowledge management, Lisbon, Portugal, 2007.
[62] G. V. Cormack, *et al.*, "Feature engineering for mobile (SMS)

spam filtering," presented at the Proceedings of the 30th annual international ACM SIGIR conference on Research and development in information retrieval, Amsterdam, The Netherlands, 2007.

Authors' information

Cik Feresa Mohd Foozy is currently working with Universiti Tun Hussein Onn Malaysia (UTHM), Malaysia. Feresa holds a Master's degree in Computer Science(Information Security) from Universiti Teknologi Malaysia, Malaysia and a Bachelor's degree in Information Technology and Multimedia from Universiti Tun Hussein Onn Malaysia (UTHM), Malaysia. She is currently pursuing her PhD at the Universiti Teknikal Malaysia Melaka, Malaysia.

Rabiah Ahmad is an Associate Professor at the Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka,Malaysia. She received her PhD in Information Studies (health informatics) from the University of Sheffield, UK, and M.Sc. (information security) from the Royal Holloway University of London, UK. Her research interests include healthcare system security and health informatics at national as well as international levels. She has also published papers in accredited information security architecture. She has delivered papers at various national/international journals. Besides that, she also serves as a reviewer for various conferences and journals.

Mohd Faizal Abdollah is an Associate Professor at the Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka,Malaysia. He received his PhD in Computer and Network Security from Universiti Teknikal Malaysia Melaka,Malaysia, and M.Sc. (Computer Science) from the University Kebangsaan Malaysia. His research interests include network and mobile security and network monitoring. He has delivered papers at various network security conferences at national as well as international levels. He has also published papers in accredited national/international journals. Besides that, he also serves as a reviewer for various conferences and journals.