Technology detection of spam SMS in mobile phones

Olorunfemi Tope Roseline

Department of Electrical and Electronic Engineering Science, University of Johannesburg, Auckland Park Kingsway Campus, 2006, South Africa

toppyrose6@gmail.com

Nwulu Nnamdi

Department of Electrical and Electronic Engineering Science, University of Johannesburg, Auckland Park Kingsway Campus, 2006, South Africa

nnwulu@uj.ac.za

Abstract

Spam is unwanted content sent electronically to many users often with the sole aim of causing monetary loss or gaining access to the user's personal information. They can either be sent via email or on mobile phones. The focus in this paper is on intrusion detection of spam Short Message Services (SMS) typically sent over a mobile telephone network. This paper therefore details the development of a mobile-based security tool application using an android studio as the platform with java programming language to detect incoming unsolicited SMSs in mobile phones. The Application (App) termed *UJ SMS Antivirus* was developed and the functionality was tested and evaluated on android mobile phones. Result shows that the proposed App is user-friendly, easy to use and can successfully filter spam SMS's.

Keywords

Detection, Mobile phones, Mobile App, Spam and SMS

1. Introduction

Spam SMSs are unwanted short messages sent electronically. Because of the low fees incurred when sending SMS. Spammers continue to send spam SMSs in bulk. The growth in mobile phone users worldwide has made them an indispensable tool/platform for efficient business transaction and personal communication. Correspondingly, this has given spammers more opportunity to exploit their evil deeds on the mobile network. An individual sending spam messages is usually called a "*spammer"* [1]. According to [2], problems relating to Spam date back to the late 1970s and its occurrence was limited to e-mail communication. However, because of

the increased penetration of internet technologies, violators now use spam as a platform for advertisement and a medium to generate illegal income. Reference [3] reveals the different platforms in which spam exists such as email, messenger, newsgroups, social network, websites and cellular phone all for the purposes of marketing, phishing and transmission of malwares. Spam is not only limited to phishing and financial gain as [4] pointed out, but spam also poses a threat on the internet for child pornography. Reference [2] predicted that the number of Smartphones users will increase from 2.6 billion in 2016 to 6.1 billion in 2020, and seven out of ten mobile phone users, do not do anything about influx of the unsubscribed messages and 44% of mobile phone users according to study did not know that there are solutions to the fake messages. In line with these there is need to research into the protection of these mobile devices by filtering the content/SMS that comes into the mobile phones. This paper presents a mobile-based security tool App developed on Android studio using Java programming language. When the App is installed on the mobile phone, it has the capability to filter messages through its various interfaces. The functionality of the developed App was tested and evaluated on Android versions 4.4 and 5.0. Results shows that the developed App is user-friendly, easy to use and can successfully detect and filter spam SMS's. The remaining sections of this paper are as follows; Section 2 presents the related works, Section 3 gives the proposed App (UJSMS Antivirus), Section 4 gives the functionalities of the App while Section 5 gives the Conclusion and future work.

2. Related works

Much research has been done in the field of SMS spam filtering. The more researchers gain grounds in their research, the more spammers devise tricks to make mobile phone users fall prey to their scams. From literatures there are basically two techniques for filtering spam SMS. The techniques are machine learning based and blacklist methods. Blacklist methods work by comparing the sender's number to a database of previously recognized spam numbers. while machine learning methods are based on classifying the content of the SMS [5]. In [6], the authors proposed a frequency ratio feature selection method to filter spam on mobile phones. The authors use Waikato Environment for Knowledge Analysis (WEKA) to break each message into keywords using the "string to word vector" in WEKA. For example, a message "As a value customer" was broken down into ["a, as, value, customer"]. The above procedure was performed on the total set of 5,574 messages. A message keyword profile matrix was generated which was used as the set of input into the machine learning tool. In reference [7], the goal was to overcome the problems of content in spam-based in SMS which are based on jargons, abbreviations and symbols. The paper proposes a "text pre-processing approach to normalize and expand the short text" in order to improve the classifiers performances when dealing with SMS messages. Their approach was based on "lexicography and semantic dictionaries" to produce a novel set of attributes to reduce redundancies and inconsistencies in words. The raw dataset involves three stages; these are "text normalization" "concept generation" and "word sense disambiguation". "Text normalization": this translates each word into the internet used language instead of English language. "Concept generation": this is used to get each possible meaning of each word. And lastly "word disambiguation": this is used to find more relevant words. So, these three stages were followed to expand the words in text to increase the classifiers performance.

Generally, SMS Spam management is in three phases: the detection phase, classification phase and filtering phase. According to [8] they could analyze the type of risks associated with each spam SMSs targeting a mobile phone. The paper further categorizes the spam into various degrees of risks and not just differentiating maybe

ham or spam. The authors use Mean Value of Content per Antigen Type (MCAT) a sub-division in the Artificial Immune Systems (AIS) theory to categorize the spam into the various degree risk levels thus: low risk will amount to low impact on user, medium risk will amount to medium risk on user and finally high risk will have high impact on users. Using the "Danger theory concept" of risk evaluation to prioritize brutality of the spam SMS, results shows that the priority severity list evaluation can be used by user to decide which spam SMS to react to and which one to ignore.

Reference [9] presents a new method for SMSs spam filtering by means of "text mining and unsupervised detection based on deep learning". Experimental outcomes show that the proposed system can filter ham from spam with high accuracy. The proposed system was compared with another filter in the literature and results show that the proposed system has greater capacity to block spam SMSs.

Reference [10] presents spam filtering by using Bayesian approach. A mobile-based SMS spam filter was developed; termed SMS Assassin which can filter spam SMSs using Bayesian learning and blacklisting method. Since the content in SMS spam keeps changing frequently by spammers, the mobile system developed also keeps updating itself through "crowd sourcing" in order to keep the system up to date. The system was tested on dataset collected manually from users. Results shows there were improvement compared to others in the literatures in terms of accuracy. The authors are also working to develop an online/cloud based spam filtering. This works such that whenever there is an incoming SMSs it will check online in the server database if it is spam or ham before it gets delivered to the user phone. According to the authors, the system is good, robust and promising to deliver mobile phone users from nuisance of SMSs spam and user privacy will not be infringed.

Reference [11] posted that the characters involved in spam SMS are generally undersized, written in slangs and contains diverse symbols. Therefore, the text representation and classification is easier said than done. Hence, they proposed "MDLText" whose idea is based on text normalization and semantic indexing. Thus, these support incremental learning and improve expert system in spam filtering.

Having critically reviewed some related works in SMS spam filtering and detection, the authors conclude that these methods in literatures are complex, often computationally and expensive to deploy on mobile phones. Therefore, there is need for state-of- the-art App which can be deployed at the mobile phone end side which is easy to use and not expensive. However, to the best of knowledge of authors this is the first of its kind ever developed App to be deployed on the mobile phone that can efficiently detect and filter SMS spam which is easy to use and user friendly.

3.0 The Application

The UJSMS Antivirus as termed is a mobile-based security tool application developed with Android studio as the platform using Java programming language. The App has the capability of detecting an incoming SMS whose number is not in the contact list of the mobile phone. Among the features of the App, it can either block or allow the SMS depending on the user's decision.

3.1 The Application flowchart

Whenever there is an incoming SMS, the system will check if the number is in the contact list of the mobile phone. If yes, the SMS will be inserted into the messaging inbox of the mobile phone; and the user will be

notified. Otherwise, if the contact is not in contact list of the mobile phone, the App will check the status of the contact. If “allowed”, it goes into the messaging inbox of the mobile phone. If the contact is blocked, it goes to end.

The flowchart for the application is given in Figure 1. A snippet of the code is also given below. For space constraints, not all the codes have been detailed.

```
// set intent so it does not start a new activity
Notification note = builder.setContentIntent(contentIntent)
                        .setSmallIcon(R.mipmap.ic_launcher)
                        .setWhen(System.currentTimeMillis())
                        .setContentTitle("New SMS Spam")
                        .setContentText("A new SMS spam has been detected!\n" + messageBody).build();
note.flags|= note.FLAG_AUTO_CANCEL;
android.app.NotificationManagermNM = (android.app.NotificationManager)
context.getSystemService(Context.NOTIFICATION_SERVICE);
mNM.notify(notifId, note);
                }else if(Contact.Status(mAddress).equals("allowed") ){
insertMessageAndNotify();
                }else if(Contact.Status(mAddress).equals("blocked") ){
//Dont do anything
Log.v("MsgReceived","This is a spam that has been blocked! don't do anything");
                }
            }else{
insertMessageAndNotify();
```

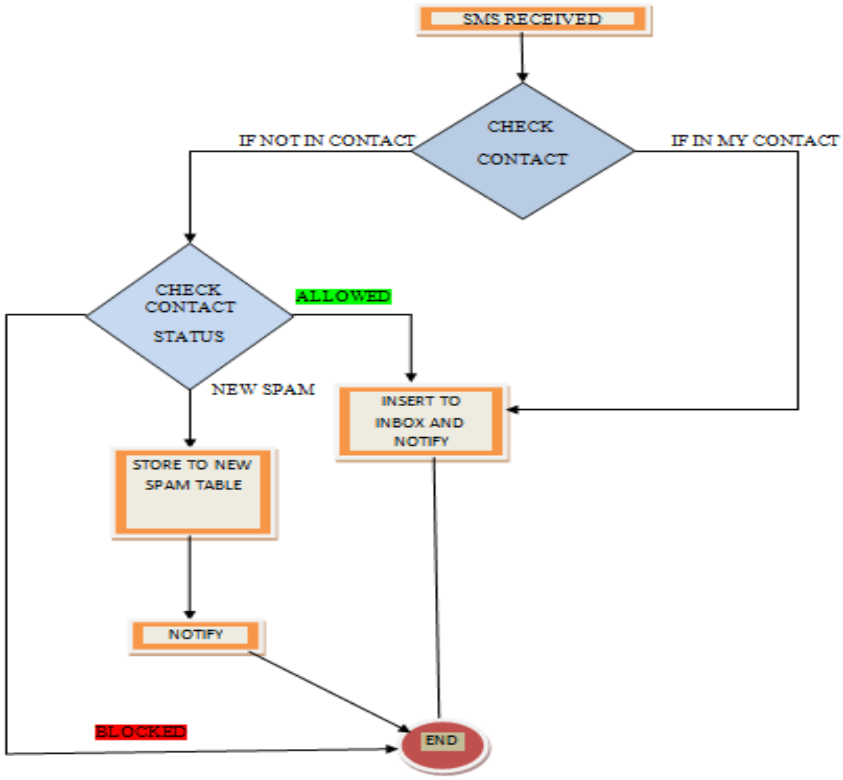

Figure 1: UJSMS Antivirus flowcharts

3.2 Evaluation and results

To test the functionality of the mobile App, the App was installed on Android mobile phone. The name of the developed App was displayed on the mobile-phone screen termed as “UJSMS”, as seen here in Figure 2.

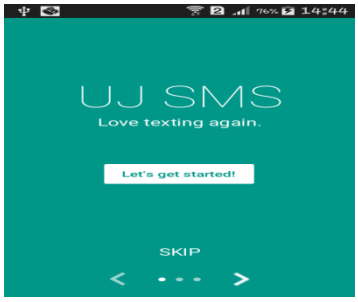

Figure 2: App successfully installed on the mobile phone

After successful installation of the App on the mobile phone, the App was set as the default messaging App of the phone as shown in Fig 3.

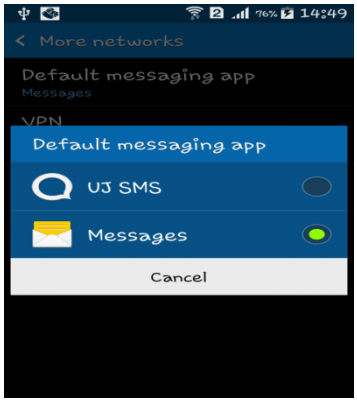

Figure 3: making the App the default messaging App

After setting the App as the default messaging App of the phone, a contact which is not in the contact list of the mobile phone is used to send an SMS to the phone. The SMS displayed at the notification bar prompting the user that there is an incoming SMS, the user taps on the SMS and the “blocked” or “allowed” option was displayed giving the user the opportunity to either allow or block the SMS. Figure 4 depicts the blocked and allowed options.

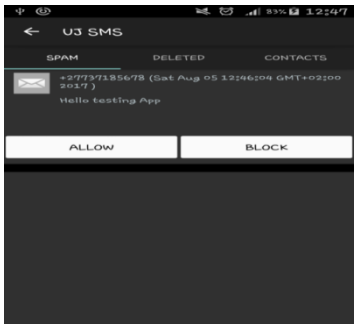

Figure 4: The allow and block option of the APP

To test the allowed functionality of the APP, a number was used to send an SMS to the phone. The SMS is displayed at the notification bar prompting the user that there is an incoming SMS, the SMS was tapped and the “blocked” or “allowed” option was displayed giving the user the opportunity to either allow or block the SMS. The “allowed” option was chosen and the SMS is delivered to the mobile phone. Figure 5 depicts end result of the allow option.

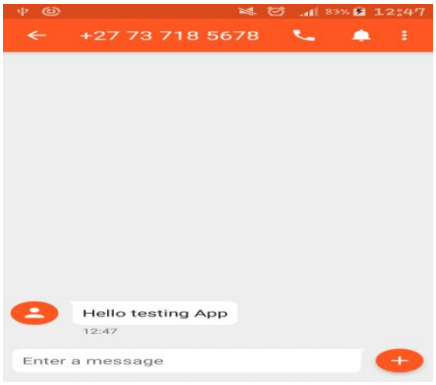

Figure 5: SMS inbox

The functionality with a known contact was used to test the App. i.e. a phone which is in contact list of the mobile phone was used to send an SMS to the phone; the SMS goes to the messaging inbox directly - without any interference or blockage as shown in in Figure 6: “Roseline TEST”

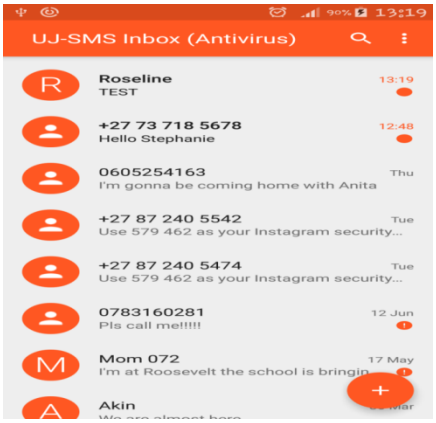

Figure 6: Testing with a known contact

4.0 Conclusion

In conclusion, a mobile application has been developed using Java programming language with Android studio as platform. The App works in a way that when installed on the mobile phone, whenever there is an incoming SMS which is not in the contact list of the phone, the App will notify the user of an incoming SMS, the user can either allow or reject the SMS. The functionality of the developed App was tested and evaluated on Android versions 4.4 and 5.0 and results shows that the developed App is user-friendly, easy to use and can successfully detect and filter spam SMS’s. While it has been established that the App is handy and would enhance user’s experience; it is therefore advisable for users who want to be safe from the influx of unsolicited SMS to get the App and install on their phone. It is easy to install and to use on mobile phones. However, it is still possible to improve the application and its use. The application is restricted to

work on selected Android versions popularly by the general populace. Therefore, it is recommended that in supplementary work; all the versions of Android so far should be covered in the developing of the App-regardless of the population and price of the device.

REFERENCES

1. Jalaluddin, K., Haider, A. and Al-Muhtadia, J. (2015) "Survey on Mobile User's Data Privacy Threat and defense Mechanism". Proceedings on International Workshop on Cyber Security and Digital Investigation. Pages 376-383
2. Templeton, B. (2015) origin of the term "spam" to mean net abuse http://www.templetons.com/brad/spamterm.html [Accessed online 12 March 2018].
3. Manajit, C., Sukomal, P., Rahul, P. and Ravindranath, C. (2016) "Recent developments in social spam detection and combating techniques: A survey" Department of computer science and Engineering, Indian Institute of Technology, India, Journal of information processing and management, Vol 53 Pages 53-73.
4. Kotenko, J. (2013). Don't click that link! http://www.digitaltrends.com/social- media/Facebook- spam-link-features-child- porn/ [Online; accessed 12 March 2018].
5. Maryam, P. and Omid, P. (2015) "Enhancing the Rate of Accuracy and Precision in Spam Filtering in Farsi SMS" Islamic Azad University Kerman Branch Computer Science Department. Communications on Applied Electronics (CAE) – ISSN: 2394-4714 Foundations of Computer Science FCS, New York, USA Volume 3.
6. Sin-Eon, K., Jung-tae, J. and Sang-Hyun, C. (2015) "SMS Spam Filtering Using Keyword Frequency Ratio" Department of Information Security Management, Department of Business Data Conversions, Department of Management Information System, Chungbuk National University 52 Naesudong-ro, Heungdeok-gu, Chungbuk 361-763 Korea. International Journal of Security and Its Applications Vol.9, No.1 Pages 329-336.
7. Tiago, P., Igor, S., Jos´e, M., G´omez, H. and Tiago, A. (2015) "Text Normalization and Semantic Indexing to Enhance SMS Spam Filtering" Department of Computer Science, Federal University of S˜ao Carlos, Sorocaba, S˜ao Paulo, 18052-780, Brazil. Universidad de Deusto, DeustoTech – Computing (S3Lab), Avenida de las Universidades 24, Bilbao, Vizcaya, 48007, Spain. Analytics Department, Pragsis, Manuel Tovar 49-53, Madrid, 28034, Spain
8. Kamahazira, Z. and Mohd Zalisham, J. "A Perception Model of Spam Risk Assessment Inspired by Danger Theory of Artificial Immune Systems" Procedia of International Conference on Computer Science and Computational Intelligence, Vol 59, pages 152-161, (2015).
9. Noura, B., Toby, B., Peter, M. and Stephen, A. "SMS Spam Filtering Using Probabilistic Topic Modelling and Stacked Denoising Autoencoder" Artificial Neural Networks and Machine Learning –Lecture Notes in Computer Science, volume 9887, Pages 423-430 (2016) Springer
10. Kuldeep, Y., Ponnurangam, K., Atul, G. and Vinayak, N. "SMS Assassin: Crowdsourcing Driven Mobile-based System for SMS Spam Filtering". Proceedings of the 12th workshop on mobile computing systems and applications, Phoenix, Arizona, March 01-02, Pages 1-6, (2011).

11. Renato, A., Tulio, A., Tiago, A. and Akebo, Y. “Towards filtering undesired short text messages using an online learning approach with semantic indexing”. Journal of Expert Systems with Applications, Volume 83, Pages 314-325, (2017).

Biographies

1. Tope Roseline, Olorunfemi is a student, teacher and security expert. She received BSc degree in Computer Science from Kogi State University, Nigeria, and Meng in Electrical and Electronic Engineering Science Department, University of Johannesburg, South Africa. She is currently pursuing her PhD degree in power systems security at the Department of Electrical and Electronic Engineering Science, University of Johannesburg. She is a member of Institute of Information Technology Professionals South Africa (IITPSA) and South African Institute of Computer Scientists and Information Technologists (SAICSIT). She has demonstrated working in the corporate industry for more than 5years before furthering her education. Strong education professional skilled in mobile App development, mathematical optimization, information security and intrusion detections.

2. Nnamdi Nwulu is a researcher, educationist and engineer. He holds BSc and MSc degrees in Electrical & Electronic Engineering and a PhD degree in Electrical Engineering. His research interests include application of mathematical optimization techniques, soft computing and energy systems. He is currently an Associate Professor in the Department of Electrical & Electronic Engineering Science at the University of Johannesburg. He is also a Professional Engineer registered with the Engineering Council of South Africa (ECSA), a Senior Research Associate in the SARChI Chair in Innovation Studies at the Tshwane University of Science and Technology and Associate Editor of the African Journal of Science, Technology, Innovation and Development (AJSTID).