Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 125 (2018) 617–623

Procedia Computer Science

www.elsevier.com/locate/procedia

6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India

Rule-Based Framework for Detection of Smishing Messages in Mobile Environment

Ankit Kumar Jain*, B. B. Gupta

Department of Computer Engineering, National Institute of Technology Kurukshetra-136119, Haryana (India) ankitjain@nitkkr.ac.in

Abstract

Smishing is a cyber-security attack, which utilizes Short Message Service (SMS) to steal personal credentials of mobile users. The trust level of users on their smart devices has attracted attackers for performing various mobile security attacks like Smishing. In this paper, we implement the rule-based data mining classification approach in the detection of smishing messages. The proposed approach identified nine rules which can efficiently filter smishing SMS from the genuine one. Further, our approach applies rule-based classification algorithms to train these outstanding rules. Since the SMS text messages are very short and generally written in Lingo language, we have used text normalization to convert them into standard form to obtain better rules. The performance of the proposed approach is evaluated, and it achieved more than 99% true negative rate. Furthermore, the proposed approach is very efficient for the detection of the zero hour attack too.

Peer-review under responsibility of the scientific committee of the 6th International Conference on Smart Computing and Communications.

Keywords: Smishing; Mobile Phishing; Data mining; Short messaging service; Machine learning

1. Introduction

These days mobile security is a major concern because attackers have diverted their mind from personal computers to smartphones because with the increase in technology. Moreover, people are more attracted towards smartphones as it is a small and multi-functioning device, Mobile devices are more popular these days as compared to laptops because of their small screen size, lower production cost, and portability.

* Corresponding author.
E-mail address: ankit.jain2407@gmail.com

1877-0509
Peer-review under responsibility of the scientific committee of the 6th International Conference on Smart Computing and Communications
10.1016/j.procs.2017.12.079

Smishing word is constructed by combining two words that are SMS and Phishing [1]. Mobile phishing is an emerging threat in which malicious person sends an SMS message to the user, and that SMS contains links to malicious applications and Webpages. The phishers will not only get money but also acquire information about contact numbers, mobile device versions, photos, etc. According to a study, 44% of users are not aware of the security solution available for mobile devices [2].

It was estimated that out of 10, seven people do not take any action against unwanted messages [3]. Attackers have now shifted their focus to mobile users due to several reasons. First is - extensive use of smartphones, second is - increase in dependency of users on smartphone applications for performing various tasks. Third, the user believes that with two-factor authentication method, only trusted messages will be delivered to their devices [5]. Multiple reports evidently indicate that Smishing attacks have dramatically increased over the last few years. In 2016, a customer of UK bank Santander lost 22,700 Pound in an SMS phishing scam [4]. According to Dimensional Enterprise Mobile security Survey report and it shows that smishing attack stands at the second position in all kind of mobile devices attacks [14].

There is two type of defense methods are used to detect fake mobile SMS. The first method is the blacklist based technique that stops the incoming SMS from the fake sources [17]. However, blacklist-based techniques do not cover all the fake sources, as a criminal can purchase any mobile number to send the bogus SMS. The second type of solution is based on the machine learning algorithm where various features are extracted and compute from the SMS to take appropriate decision. The advantage of the machine learning based technique is that it can detect the fake message coming from any source. Data mining methods help in the feature extraction and finding the relation between them [16]. These approaches identifying hidden knowledge from datasets in terms of rules and make the decision based on extracted rules. Human easily understands these rules and their rules are written in the form of IF-condition THEN action.

In this paper, we employed the rule-based data mining classification approach in the prediction of smishing SMS. We study the various characteristics of text messages in depth and then found nine rules which can efficiently filter smishing SMS to the legitimate one. We then use rule-based classification algorithm namely Decision Tree, RIPPER and PRISM to apply these rules. In this, we have also identified the minimal effective feature set in the detection of smishing messages. Moreover, we recognise the best rule-based classification algorithm in the classification of smishing messages. The performance of the proposed approach is evaluated, and it achieved more than 99% of true negative rate and 92% true positive rate.

The rest of the paper is organized as follows. Section 2 presents the related work. Section 3 presents the overview of the rule-based approach. Section 4 presents the experimental evaluation. Finally, Section 5 concludes the paper and present the future work.

2. Related Work

This section discusses the various existing mobile phishing detection techniques. The existing mobile phishing detection techniques divide into following categories.

2.1. User Education Based Schemes

The educational based solutions emphasis on educating the mobile users about the characteristics of phishing message through training, workshop and awareness programs so that they correctly identify the phishing attack [8]. However, the phishing attack becomes successful due to human flaws and ignorance. This conceptual knowledge may help the users in avoiding phishing attacks.

2.2. Technical solutions to mitigate mobile phishing attack

The technical solutions are also cost-effective and easy to implement (driven and download) as compare to educational based solutions. In this, Amrutkar et al. [9] proposed a mechanism named KAYO, which differentiates between the malicious and genuine mobile webpages. It detects mobile malicious pages by measuring 44 mobile

features from webpages. Out of these 44 features, 11 are newly identified mobile specific features. KAYO's 44 feature set is divided into four classes namely HTML, mobile specific, URL and JavaScript features.

Joo et al. [6] proposed a model 'S-Detector' for detecting Smishing attack. They used Naïve Bayesian Classifier in their system to filter Smishing messages by finding the words used more often in these messages. S-Detector consists of SMS monitor, SMS analyzer, SMS determinant, and Database. Foozy et al. [7] proposed a rule-based methodology to filter out smishing messages from spam messages. Authors applied two rules namely 'winner announcement' and 'marketing advertisement'. They have applied the Bayesian technique in WEKA tool to check the accuracy of Smishing, spam and ham messages. Alfy et al. [15] proposed a spam filtering model for both email and SMS. The proposed technique used 11 features namely presence of URLs, likely spam words, emotion symbols, special characters, gappy words, message metadata, JavaScript code, function words, recipient address, subject field and spam domain. They have evaluated their proposed model on five email and SMS datasets.

In the literature, we can conclude that no single technique exists that can detect smishing attacks efficiently. Therefore, we need a technique that can protect the user against smishing attacks.

3. Proposed Rule-Based Approach

In this section, we discuss our proposed of smishing detection model. The proposed approach is a security model that protects the user from the phishing SMSs by blocking these messages and delivering only Normal ones to the mobile user. The smishing detection is a type of binary classification problem where a message can be the divide in two categories (i.e., smishing and legitimate). Smishing message is a harmful spam message that steals personal credentials. As per our observation, we find the followings characteristics of Smishing message:

- It contains the bogus fake links, email address or a cell number.
- Advertising something like providing free minutes, etc.
- Self-answering SMS asking the user to subscribe or unsubscribe any service.
- Announcing user as a winner of some fake contest and luring him using the prize money.
- Intended to spread some fake news.

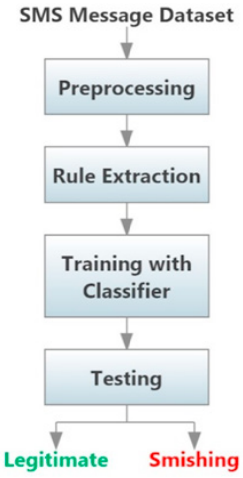

Fig. 1. Architecture of the Proposed Approaches

We have considered these characteristics while making the proposed rule set. Figure 1 presents the system architecture of the proposed approach. The proposed approach contains following three phases.

Preprocessing - Pre-processing the entire SMS Corpus to remove the redundancy. Preprocessing recognizes boundary of sentences, tokenization, auto word spacing, and lowercase text conversion. The output of this phase is normalized and unambiguous text that makes further processing of the text easier for the upcoming phases.

Rule Extraction- A rule extractor identifies the useful rules which can be useful in the classification process and extract these rules from the SMS. A feature vector value 1 is set for smishing message and 0 for legitimate message for each rule in rule set.

Classifier Training and Testing - The labeled dataset is being used for testing and training purpose. The cross-validation set improves the parameters, and it is used to test the accuracy of the model. After training and testing, we get results in two classes namely smishing and legitimate.

3.1. Proposed Rule Set

Rule selection is an essential task for the smishing filtering. Selected rules should be correlated to the message type such that accuracy for detection of smishing message can be increased. There is a length limit for SMS message, and it contains only text (i.e., no file attachments, graphics, etc.) while in the email, there is no text limit and it includes attachments, graphics, etc. This section explains the various rules employed by our approach in the classification of smishing and legitimate messages. A rule is generally written in the form of IF condition THEN action. It means if the condition is fulfilled then the action is of that specific rule is implemented. The rules, which are used in the proposed approach, summarized as follows: -

Rule 1: If URL present in the message, THEN it is probably a smishing message. A URL analyzer checks for the presence of URL in the text message since attackers can trick users by sending a URL link in the text message which when opened can direct the user to either a malicious login page or can download a malware in the user's mobile phone.

Rule 2: If the message contains any mathematical symbol like +, -, <, >, /, etc., THEN it is a probably a smishing message.

Rule 3: IF message contains any currency sign like "$", "£", etc., THEN it is a probably a smishing message. For example, specific symbol "$" is being used to represent money in the fake award messages. We have selected two symbols frequently present in the smishing message namely $ (Dollar) and £ (Pound).

Rule 4: IF mobile number present in the message, THEN it is a probably a smishing message. The attacker asks the users to send the user's details, bank details, on given number.

Rule 5: The presence of suspicious keywords like, free, accident, awards, dating, won, service, lottery, mins, visit, delivery, cash, claim, Prize, delivery, etc. are considered as smishing keywords. If any of the suspicious keyword present in the message, THEN it is a presumably a smishing message.

Rule 6: IF message length is greater than 150 character, THEN it is potentially a smishing message. This length including space, symbols, special characters, smileys, etc.

Rule 7: IF message is the self-answering type, THEN it is a likely a smishing message. The presence of self-answering SMS asks the user to subscribe or unsubscribe any service.

Rule 8: IF message contains visual morphemes, THEN it is probably a smishing message. Visual Morphemes are numerals and other signs used in writing text messages or emails etc.

Rule 9: IF message contains the e-mail address, THEN it is likely a smishing message. The attacker also uses the email address in the message to get the personal information on the desired source.

4. Experimental Evaluation

This section describes the experimental dataset and various results to validation of our approach on the dataset of smishing and legitimate messages.

4.1. Dataset Preparation

Until now, benchmarked smishing dataset is not publically available. Smishing messages are the subset of the spam messages. A spam message is an unwanted message like free services, promotions, advertisements, etc. whereas Smishing message is bad spam message which intends to steal personal and financial information of the user. Therefore, we have manually filter smishing messages from the spam messages. The SMS Spam dataset v.1 is collected from SMS Spam research work [10]. This dataset contains 5574 text messages in the English language labeled as ham and spam. In the pre-processing, we filter the smishing message from spam. After pre-processing, our final dataset contains 5169 message of which 362 are smishing messages, and 4807 are the ham messages.

4.2. Evaluation of proposed rules

Figure 2 present the histogram of Rules 1-9 taken on spam v.1 dataset. From figure 2, we observed that rule 3,4 and 5 are great sign of smishing messages and frequently satisfy smishing messages. Moreover, these three rules can correctly filter more than 90% of smishing messages and 99% legitimate messages. Rule 7 and 9 fulfill some smishing messages (Approximate 7% and 2%), while only 20 and 3 legitimate message satisfies these rules. Moreover, 48.34% of smishing messages and 10.30% of legitimate messages satisfy the rule 6. Furthermore, Rule 1, 2 and 8 satisfy 28.45%, 53.59% and 3.39 % smishing messages respectively.

The histogram in Figure 3 shows rule count from 0 up to 9. Figure 3 shows that most of the smishing message satisfies at least 2 rules and none of the smishing messages satisfy more than 6 rules. This histogram is used to choose the appropriate threshold to filter the smishing message accurately. One naïve approach is assigned the weight to each rule and calculate the number of rules fulfilled by a message. If weight count of total number rules for a message is higher than the defined threshold, the message considers as smishing. The appropriate threshold should detect more number of smishing messages (i.e., high true positive rate and low false negative rate).

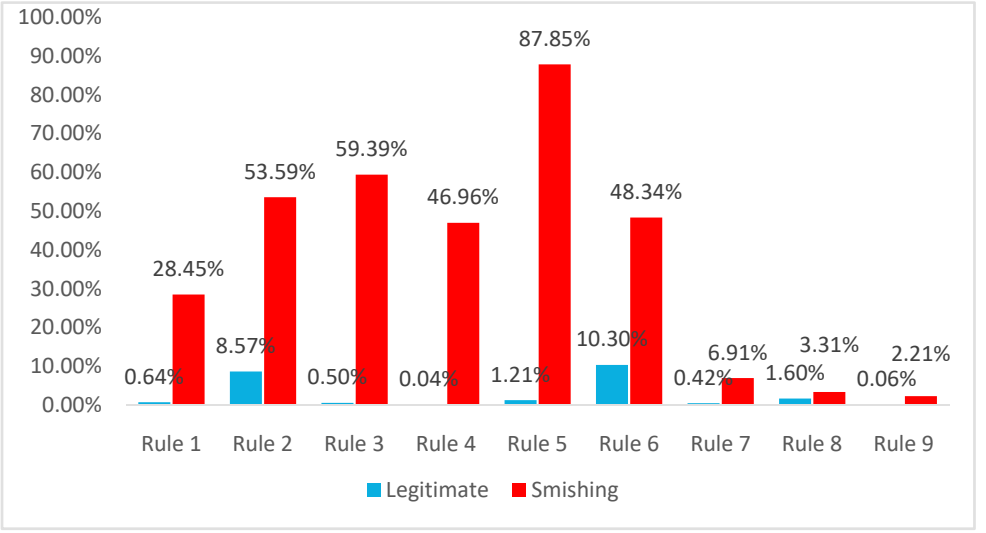

Fig. 2. Histogram of Rule1-Rule9 on dataset

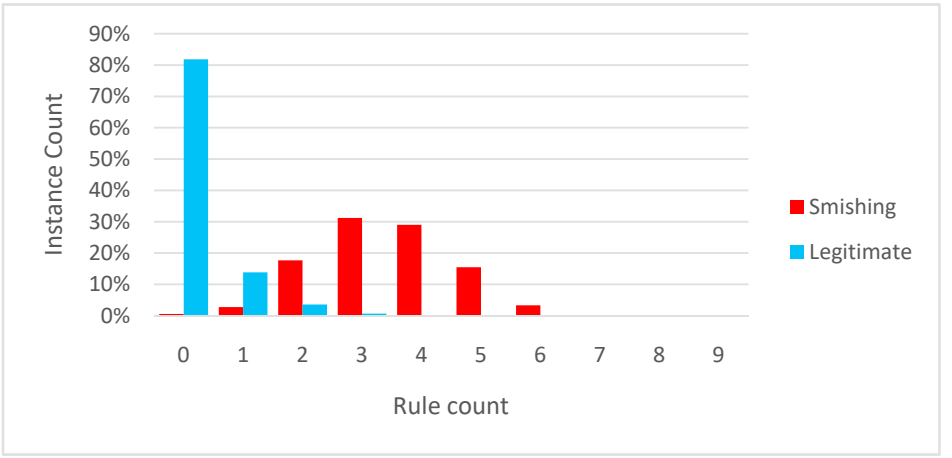

Fig. 3. Histogram of rule count

4.3. Implementation of rule-based classification algorithm

A desktop machine having core Pentium i5 processor with 2.4 GHz clock speed is used to conduct experiments. WEKA software is used to judge the performance of proposed technique on various classifiers. We have implemented four rule based classification techniques namely Decision Tree (DT), RIPPER, and PRISM. The DT [11] is tree structure based which is based on divide-and-conquer techniques. The RIPPER [12], which implements a separate-and-conquer method. The PRISM [13] algorithm is based on new induction algorithm, and it yields the results as a set of modular rules. Table 1 present the result of our approach on various rule-based classifiers. The results exposed that RIPPER outperforms DT and PRISMS in term of high TPR. The PRISM algorithm received highest TNR, but its FNR is very high (27.35%). The Decision tree received considerable TRP and TNR. The overall result shows that the proposed rules are efficient in the filtering of smishing and legitimate messages. Figure 4 presents the decision tree model.

```
R5 = 0
|  R4 = 0: 0 (4773.0/24.0)
|  R4 = 1: 1 (20.0)
R5 = 1
|  R4 = 0
|  |  R1 = 0
|  |  |  R3 = 0
|  |  |  |  R2 = 0
|  |  |  |  |  R7 = 0: 0
(35.0/8.0)
|  |  |  |  |  R7 = 1: 1 (4.0)
|  |  |  |  R2 = 1: 1 (21.0/7.0)
|  |  |  R3 = 1: 1 (90.0/23.0)
|  |  R1 = 1: 1 (76.0/1.0)
|  R4 = 1: 1 (150.0)
```

Fig. 4. Decision Tree Model using C.5 Algorithm

Table 1. Result of the Proposed Approach

Algorithm	True Positive Rate	True Negative Rate	False Positive Rate	False Negative Rate
Decision Tree	90.88%	99.17%	0.86%	9.12%
PRISM	72.65%	99.93%	0.07%	27.35%
RIPPER	92.82%	99.01%	0.99%	7.18%

5. Conclusion and Future Work

In this paper, a novel rule-based approach to detect smishing SMS is proposed. We had study the properties of smishing SMS and identified the nine outstanding rules to catch these harmful messages. These rules are extracted from the content of the message. The experiments results showed that the RIPPER outperformed Decision Tree and PRISM in terms of TPR. Proposed rules received a TNR of more than 99% in all the algorithm. Moreover, our approach can also detect the zero-day attack. In our future research work, we plan to introduce new and meaningful rules that can improve the TPR and overall accuracy of the approach. Moreover, we are collecting dataset manually from various institutes, companies, and bank organization for real-time detection.

References

1. N. Choudhary and A.K. Jain, Comparative Analysis of Mobile Phishing Detection and Prevention Approaches, *International Conference on Information and Communication Technology for Intelligent Systems*, pp. 349-356, (2017).

2. Symantec Internet Security Threat Report, Available at: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf. Accessed August 2017
3. Mobile messaging fraud report, Available at: https://mobileecosystemforum.com/mobile-messaging-fraud-report-2016/.
4. Smishing Report, Available at : http://resources.infosecinstitute.com/category/enterprise/phishing/phishing-variations/phishing-variations-smishing/, last accessed 2017/07/15.
5. The Social Engineering Framework, Available at: https://www.social-engineer.org/framework/attack-vectors/smishing/.
6. J.W. Joo, S.Y. Moon, S. Singh and J.H. Park, S-Detector: an enhanced security model for detecting Smishing attack for mobile computing, Telecommunication Systems vol. 66(1), 29–38 (2017).
7. M. Foozy, C. Feresa, R. Ahmad and M.F. Abdollah, A practical rule based technique by splitting SMS phishing from SMS spam for better accuracy in mobile device, International Review on Computers and Software, vol. 9(10), pp. 1776-1782 (2014).
8. A. Tewari, A. K. Jain and B. B. Gupta, Recent survey of various defense mechanisms against phishing attacks. Journal of Information Privacy and Security, 12(1), 3-13, 2016.
9. C. Amrutkar, Y.S. Kim and P. Traynor, Detecting Mobile Malicious WebPages in Real Time, *IEEE Transactions on Mobile Computing* (2016)
10. T. A. Almeida, J. M. G. Hidalgo and A. Yamakami, Contributions to the study of SMS Spam Filtering: New Collection and Results, *In 11th ACM Symposium on Document Engineering (ACM DOCENG'11)*, pp 259-262 (2011).
11. J. R. Quinlan, C4. 5: programs for machine learning. Elsevier, (2014).
12. W.W. Cohen, Fast effective rule induction*, In Proceedings of the twelfth international conference on machine learning*, pp. 115-123, (1995).
13. [13] J. Cendrowska, PRISM: An algorithm for inducing modular rules. International Journal of Man-Machine Studies, vol. 27(4), pp. 349-370 (1987).
14. Dimensional Enterprise Mobile security Survey, Available at: http://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Sury.pdf.
15. E. M. El-Alfy and Ali A. AlHasan, Spam filtering framework for multimodal mobile communication based on dendritic cell algorithm, Future Generation Computer Systems, vol. 64, pp. 98-107, (2016).
16. N. Choudhary and A.K. Jain, Towards Filtering of SMS Spam Messages Using Machine Learning Based Technique. *Advanced Informatics for Computing Research,* 18-30, 2017.
17. A. K. Jain and B. B. Gupta, A novel approach to protect against phishing attacks at client side using auto-updated white-list. *EURASIP Journal on Information Security*, 2016(9), 2016.