ISSN: 0067-2904

Review of Smishing Detection Via Machine Learning

Ameen R. Mahmood*, Sarab M. Hameed
Department of Computer Science, University of Baghdad, Baghdad, Iraq

Received: 23/8/2022 Accepted: 4/11/2022 Published: 30/8/2023

Abstract

Smishing is a cybercriminal attack targeting mobile Short Message Service (SMS) devices that contains a malicious link, phone number, or email. The attacker intends to use this message to steal the victim's sensitive information, such as passwords, bank account details, and credit cards. One method of combating smishing is to raise awareness and educate users about the various tactics used by SMS phishers. But even so, this method has been criticized for becoming inefficient because smishing tactics are continually evolving. A more promising anti-smishing method is to use machine learning. This paper introduces a number of machine learning algorithms that can be used for detecting smishing. Furthermore, the differences and similarities among them as well as the pros and cons of each are presented to support future research into more effective anti-smishing solutions for securing mobile devices from cyber criminals.

Keywords: anti-smishing, heuristic, machine learning, phishing, smishing.

دراسة حول كشف التصيد عبر الرسائل النصية القصيرة بوساطة التعلم الالي

امين رحمان محمود*، سراب مجيد حميد
قسم علوم الحاسوب، جامعة بغداد، بغداد، العراق

الخلاصة

التصيد الاحتيالي عبارة عن هجوم اجرامي الكتروني يستهدف رسائل اجهزة الهواتف المحمولة والتي تحتوي على رابط الكتروني او رقم هاتف او بريد الكتروني ضار. يعتزم المهاجم استخدام هذه الرسالة لسرقة المعلومات الحساسة للضحية، مثل كلمات المرور وتفاصيل الحساب المصرفي وبطاقات الائتمان تتمثل إحدى طرق مكافحة التصيد الاحتيالي في زيادة الوعي وتثقيف المستخدمين حول الأساليب المختلفة التي يستخدمها المتصيدون عبر الرسائل النصية القصيرة.

ولكن رغم ذلك، تم انتقاد هذه الطريقة لأنها أصبحت غير فعالة لأن تكتيكات التصيد الاحتيالي تتطور باستمرار.هناك طريقة واعدة لمكافحة التصيد الاحتيالي وهي استخدام التعلم الآلي. يقدم هذا البحث عددًا من خوارزميات التعلم الآلي التي يمكن استخدامها لاكتشاف الاحتيال الإلكتروني. علاوة على ذلك، يتم تقديم الاختلافات والتشابهات والإيجابيات والسلبيات لكل منها لدعم البحث المستقبلي في حلول مكافحة التصيد الاحتيالي الأكثر فعالية لتأمين الأجهزة المحمولة من مجرمي الإنترنت.

*Email: Ameen.rahman1201a@sc.uobaghdad.edu.iq

1. Introduction

Mobile phone usage has increased which has led to an increase in cybercrime. Smishing is one such crime. It is a type of spam that has a significant negative impact on many users' daily lives. They waste a lot of time processing spam that contains unexpected dangerous attachments to compromise the users' systems [1]. Information security is a major concern in our daily life that deal with controlling and preventing unauthorized access to secure data [2].

Phishing is currently one of the serious risks to human networking environments. It is a cybercrime that sends malicious links via spam or social network to trick users into gaining access to personal information such as usernames and passwords. Phishing scams can allow attackers to make money or other profits [3]. Smishing is phishing carried out through a Short Message Service (SMS) to steal user-sensitive information. In smishing, the attackers target mobile users via text messages delivered to their mobile. These messages include a link to malware or phishing websites that will request sensitive data from the user. Malware is downloaded to the mobile of the user and then performs malicious operations on the device. Attackers prefer text messages to target victims because they can aim for a huge number of users with an inexpensive SMS subscription [4]. Furthermore, the mobile phone has a smaller display that makes it hard for users to read the Uniform Resource Locator (URL) and review the suspicious features of that particular URL. In addition, mobile users' lack of knowledge, insecure user behavior, and frequent user logins make mobile phones vulnerable to smishing attacks and loss of sensitive data.

This paper presents a detailed study of anti-smishing techniques for mobile device security. The review's main contribution can be summarized as follows:

- Present a review of the main and most recent research advancement of anti-smishing methods in the literature with their drawbacks and results.
- Investigate potential solutions to smishing attack problems from various perspectives such as collaboration among SMS content, URL analysis, and the combination of URL analysis and SMS content.

For the rest of this paper, the smishing mechanisms are described in section 2. Section 3 presents various anti-smishing techniques. Followed by a discussion. Finally, the major findings of this review are clarified

2. Smishing mechanisms

Smishing operations created by attackers usually use compelling phrases such as congratulations, wins, prizes, gifts, etc. This tricks the user into contacting the attacker by clicking the link, dialing the phone number, or contacting the email provided in SMS. The process of a smishing attack, as shown in Figure 1, begins with an SMS message from the attacker containing one of three: a URL, Email ID, or phone number. If the URL is included in the SMS, simply clicking the link will redirect the user to a dangerous website. Next, a website form for the victim is opened, containing a gift and a promise about the customer's points of interest. The victim will be asked to enter personal information such as bank information to obtain this. On the other hand, the malicious message may contain a website link that redirects the victim's device to download a file.

For SMS containing an email ID or phone number, the attacker calls the phone number or email ID to trick the victim into contacting them. If the victim contacts the attacker in any way, the attacker will ask the user to disclose personal information [4, 5]. Figure 2 depicts four examples of smishing.

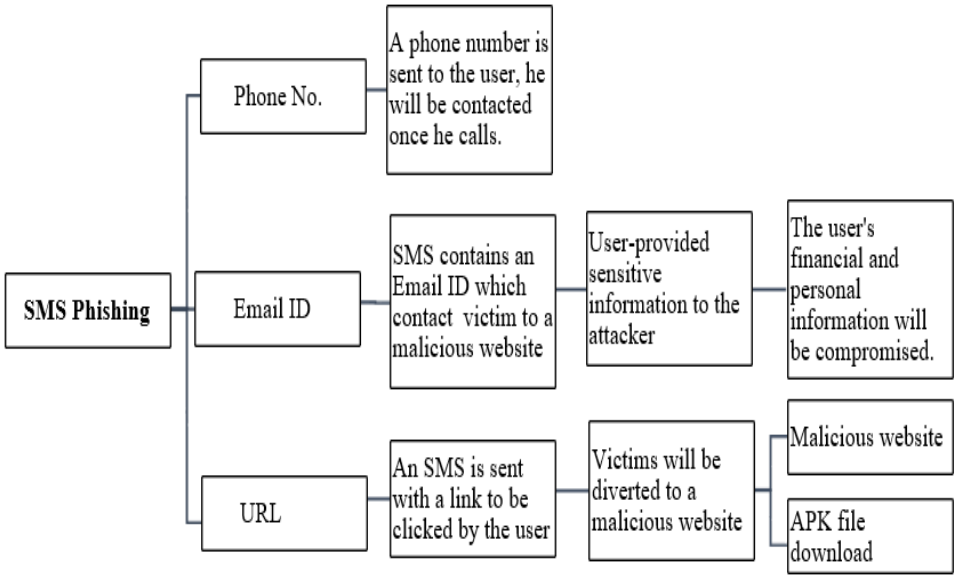

Figure 1: Smishing malicious activities

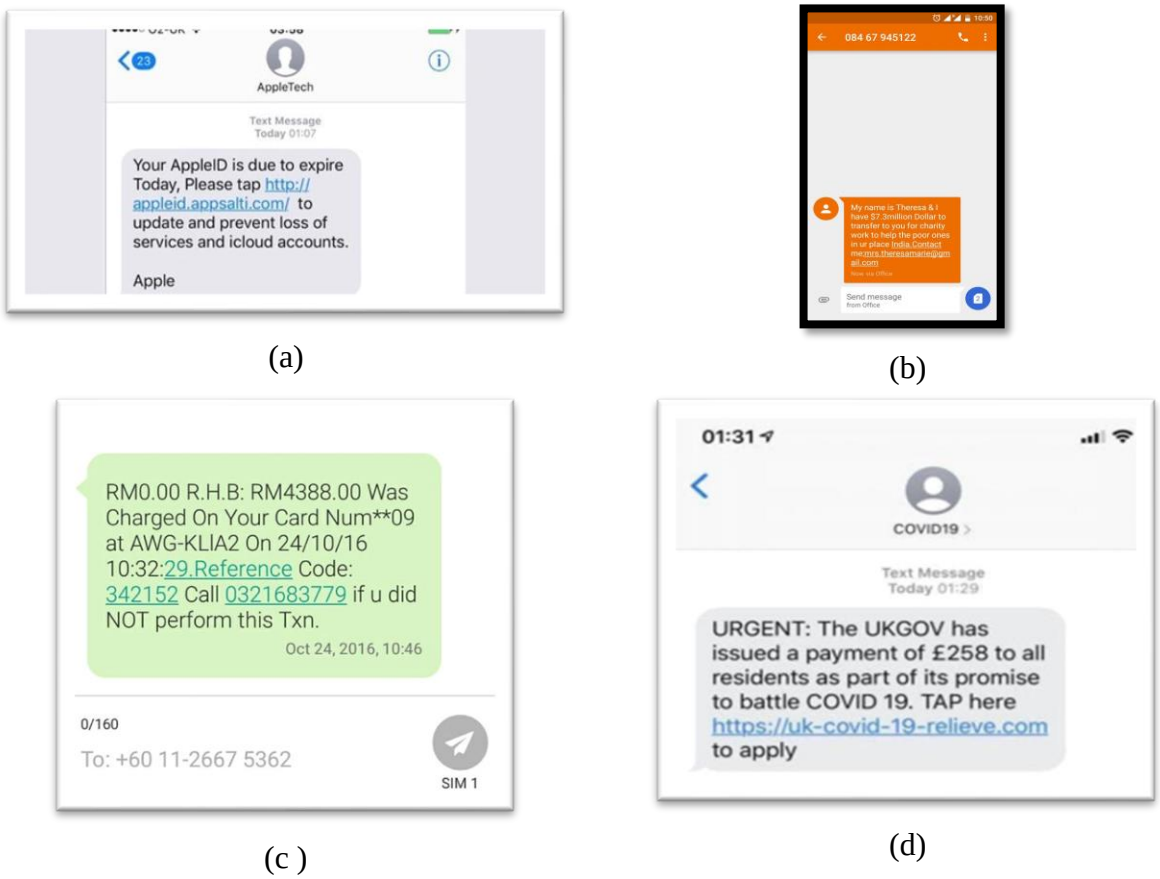

Figure 2: Examples of smishing messages. (a) Smishing contains a warning about AppleID. (b) Smishing using E-mail ID. (c) Smishing by phone number. (d) a malicious message contains an urgent warning assuming that it is sent by the UK government

3. Anti-Smishing techniques

Researchers have proposed several approaches to combat smishing attacks, including content-based, URL behavior analysis, and heuristic techniques. Figure 3 depicts the distribution of the three existing approaches for all publications presented in this review.
A smishing system was suggested by Joo et al. [6] to detect and block smishing messages by checking if a URL exists in the message. The system consists of four parts: SMS monitor, analyzer, determinant, and database. Finally, the system can efficiently extract noun words using a morphological analyzer, Naïve Bayesian classifier was used to classify smishing messages from legitimate ones.

A smishing detection model that relies on a combination of content-based and four well-known machine-learning algorithms for detecting smishing messages was proposed by Sonowal and Kuppusamy [7]. To minimize the number of features and the dimensionality reduction method, the Pearson correlation coefficient was used to extract 39 features and the 20 best features were selected. The model was validated by experiments on both the English and non-English datasets. The model's accuracy, when applied to an English dataset, was 96.40%, while it was 90.33% when applied to a non-English dataset. The model obtained a 96.16% accuracy after feature selection.

A rule-based technique with content-based filtering was presented by Jain and Gupta [8]. The authors proposed nine rules and three algorithms: Repeated Incremental Pruning to Produce Error Reduction (RIPPER), decision tree, and PRISM to classify smishing messages from legitimate messages. The obtained results were promising and the proposed method could also detect the zero-day attack. In terms of True Positive Rate (TPR), the RIPPER outperformed DT and PRISM, which showed 90.88% and 72.65%, respectively. In terms of True Negative Rate (TNR), the RIPPER showed 99.01%, while the DT and PRISM obtained 99.17% and 99.93%, respectively.

Goel and Jain [9] proposed a three-phase smishing detection model. The first phase is the SMS analysis phase, in which the URL analyzer checks for the presence of URLs in text messages, the mobile number analyzer checks whether the phone number in the SMS is on the blacklist, and the self-answering message analyzer searches for messages that require a "yes" response to register for a service. The second phase is SMS normalization, which replaces normalized disguised noisy text with its familiar form. The third phase is SMS classification, which includes preprocessing and classification using Nave Bayesian (NB) classifier.
Wu et al. [10] proposed an anti-smishing framework with three types of features: 32 token features, 50 topic features, and 93 LIWC features. To resolve the imbalanced data, the adaptive Synthetic (ADASYN) oversampling method was used. Because there were so many features, the Binary Particle Swarm Optimization (BPSO) method was used to reduce the dimensions of the features and identify feature combinations. For distinguishing smishing from legitimate messages, the RF classification method was used. In terms of accuracy, the proposed technique achieved 99.01%.

A technique based on the message content and URL behavior analysis for detecting smishing was introduced by Mishra and Soni. [4] They proposed a Smishing detection system using SMS content analysis, a machine learning classifier, and the inspection of the URL behavior method to classify the smishing messages. The first phase filters the content of text messages by detecting the presence of email IDs, phone numbers, or URLs in messages. Word occurrences were calculated using the term Frequency-Inverse Document Frequency (TFIDF) and OneVsRest classifier to distinguish between smishing and legitimate messages. Analyzing URL

behavior can help detect APK downloads. Meanwhile, the URL source code is also determined to see if the form tag is present in the message.

[11] proposed a content-based technique known as automatic detection of smishing using machine learning algorithms using Support Vector Machine (SVM), Logistic Regression (LR), and Random Forest (RF). The core of the proposed work consists of preprocessing, feature extraction, and classification. To assess the performance of the proposed model, a large dataset containing smishing and legitimate messages was used. The experimental results clarify that legitimate and smishing messages were classified with a high success rate. SVM, RF, and LR classifiers achieve precision of 88%, 88%, and 89%, recall of 98%, 98%, and 96%, and F1-score of 92.7%, 92.7%, and 92.4%, respectively.

Jain and Gupta [12] proposed a heuristic-based algorithm that detects smishing messages using feature selection and machine learning algorithms. Ten features from the smishing message were selected by analyzing the content of the message and using a classification algorithm to distinguish the messages depending on the selected features. The suggested algorithm has an overall accuracy of 98.74%, a TPR of 94.20%, and a TNR of 99.08% for smishing detection using an RF classifier.

A smishing detector was proposed by Mishra and Soni based on a content-based approach and a URL-based method. The system consists of four modules. The content of the message was processed by the SMS Content Analyzer. URL filters, APK downloads, and source code modules for examining URL behavior. The naive Bayes classifier was used as a machine-learning algorithm to classify smishing messages from legitimate messages and showed an accuracy of 96.29% after the evaluation of all four models [13].

A combination of the heuristic method and content-based feature extraction with machine learning classifiers namely naive bays (NB), neural network (NN), and LR to detect smishing messages was introduced by Jain et al. [14]. The system was divided into two phases. In the first phase, spam and ham messages were filtered. Then in the second phase, the smishing messages were distinguished from spam messages. This approach can detect both spam and smishing messages. The proposed approach used 11 basic features to exclude spam messages and 4 features to filter smishing messages with the use of Information Gain (IG) for feature selection to reduce redundancy. The simulation results show that using a NN classifier, the proposed method can recognize spam messages with an accuracy of 94.9% and identify smishing messages with an accuracy of 96%.

Sonowal [15] proposed a detecting smishing messages based on content feature extraction and four correlation machine learning algorithms namely spearman's correlation, Pearson rank correlation, point biserial rank correlation, and Kendall rank correlation for ranking features. The Kendall ranking algorithm reduced feature dimension by 61.53% and achieved an accuracy of 98.40%. using AdaBoost classifier.

Mishra and Soni [16] offered a smishing detection model that consists of two phases: the domain checking phase and the SMS classification phase. The first one looks at the authenticity of the SMS URL, which is an important part of SMS phishing detection. The second phase is the SMS classification phase, which looks at the textual content of the message and chooses the five most effective features from the text messages to allow machine learning categorization with a small number of features. Finally, the proposed system classifies messages using Backpropagation (BP) algorithm, RF, NB, and DT. The obtained accuracy was 97.93%.

A smishing detection model based on a content-based approach was developed by [17]. They have developed an automated strategy that effectively distinguishes between legitimate and fake messages. They performed a feature extraction method, followed by a feature selection method, and analyzed the work by machine learning classifiers XGBoost, RF, Classification and Regression Tree (CART), SVM, and AdaBoost. SVM outperforms the others with accuracy, precision, recall, and F1-scores of 98.39%, 98.37%, 99.79%, and 99.08%, respectively.

A content-based approach used artificial intelligence for smishing detection. First, the message is preprocessed and features such as (term function, URL, email address, mobile number, number of characters, and currency symbol) are extracted. These features are provided to the classifier for distinguishing the smishing message from the original message. Many classifications such as Long Short-Term Memory Recurrent Model (LSTM), K-neighbors (KNN), stochastic gradient descent (SGD), DT, NB, and RF classifiers were used and it was found that LSTM achieved 95.11%, 94.88%, 91.07% and 99.03% for accuracy, F1-score, recall, and precision respectively [18].

Ghourabi [19] proposed an "SM Detector" for smishing detection in the mobile environment. This system consists of three parts. The first uses the VirusTotal API to analyze the authenticity of the URL, and the second uses the regular expression technique to analyze the content of the message for blacklisted words or numbers. The last part was the Bert classification method for classifying spam messages from original messages. The system also includes a mobile app that allows users to monitor their SMS and report smishing texts. Its main advantage is that it can handle mixed text messages written in Arabic or English. On both Arabic and English datasets, the accuracy was 99.63%.

A smishing detection model based on a content-based approach was developed by Boukari et al. [20], they developed an automated strategy that effectively distinguishes between legitimate and fake messages. They performed a feature extraction method, followed by a feature selection method, and analyzed the work using machine learning classifiers. SVMs are the best in achieving superior accuracy and reducing feature dimensions. The method can also detect phishing and vishing scams.

An SMS phishing detection technique was proposed by Mishra and Soni [5] that used a neural network to extract 7 significant features and it showed the best results for detecting smishing. The overall accuracy of the NN-based 'Smishing Detector' model outperforms the results of the same model using machine learning methods. The comparison shows that the NN achieved greater accuracy, with a 1.11% difference. The NN achieved 97.40% accuracy and TPR and TNR of 92.37% and 97.91%, respectively.

Akande et al. [21] proposed a mobile application for detecting smishing attacks based on rule-based RIPPER and C4.5 classifiers. The rule-based classifiers were used to generate rules for identifying and distinguishing spam from ham, and a mobile application was developed to use the rule-based approach to detect smishing. An Application Programming Interface (API) was developed to intercept incoming SMS. The use of the C4.5 PART algorithm improved the efficiency of the rule-based method significantly. The correct classification rate was determined to be 98.42 %. However, 1.58 % of cases were labeled incorrectly.

Phadke and Thorpe [22] developed a new app to detect Smishing attacks on Android smartphones by incorporating current phishing Application Program Interfaces (APIs) into a

prototype application. The system is designed to run in the background and determine whether the URL in the text message is phishing or not. Five freely available APIs were tested on a 1500 URL dataset to determine their accuracy and latency. The VirusTotal API has the highest detection rate of 99.27% with a response time of 12-15 seconds per query for the security sensitive application. Furthermore, for the time-sensitive application, the Safe-Browsing API has an 87% accuracy and a response time of 0.15ms.

A technique was offered by Mambina et al. [23] that used a machine-learning-based approach for classifying smishing SMS messages. The best model with an accuracy score of 99.86% was a hybrid model of Extra tree classifier feature selection and RF employing TF-IDF (Term Frequency Inverse Document Frequency) vectorization. The results obtained were compared to a baseline. multinomial Nave-Bayes model. Furthermore, a comparison with a group of other classifiers was performed. As a result, the lowest false positive and false negative were 2 and 4, respectively the model provides with a Log-Loss of 0.04.

Jain et al. [24] presented an effective method for analyzing text content and URL in SMS. They combined the URL phishing classifier with the text classifier to increase accuracy because some SMS include the URL with no or very little content. A weighting framework TF-IDF was used to locate unusual terms in a report, two datasets were used in the system for text and URL phishing classifier. Also, to balance the training data, an oversampling method was introduced. The proposed system was able to detect smishing SMS with 99.03% and 98.94% accuracy and precision rate respectively.

Figure 4 shows how many times classifiers were used in different research papers from 2017 to 2022. It demonstrates that the most commonly used classifier is random forest.
Table 1 presents comparative studies by various recent researchers from different perspectives based on the approach, dataset, feature extraction, feature selection, and classifier used, followed by the results and limitations.

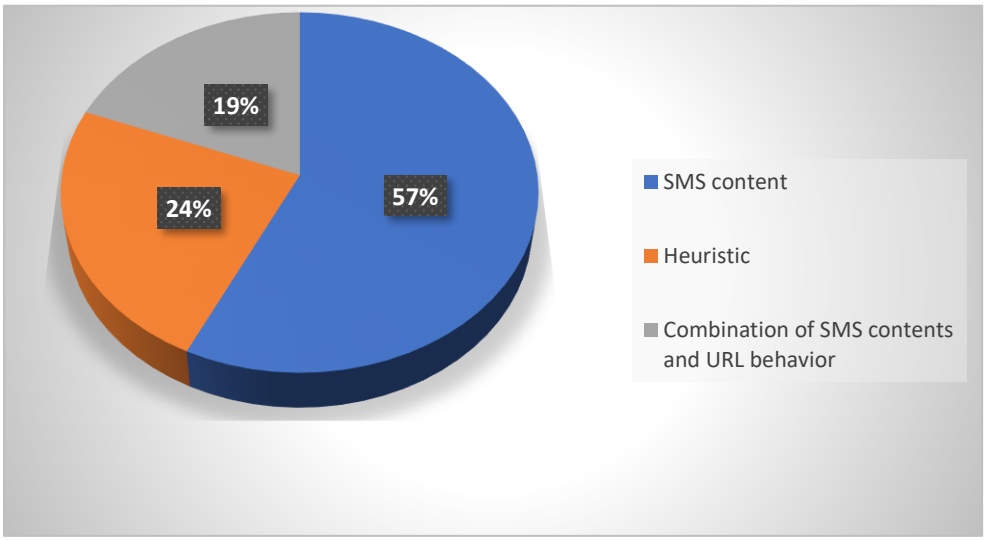

Figure 3: Distribution of anti-smishing using three approaches (SMS contents, Heuristic, and combination of SMS contents and URL) during the period 2017-2022

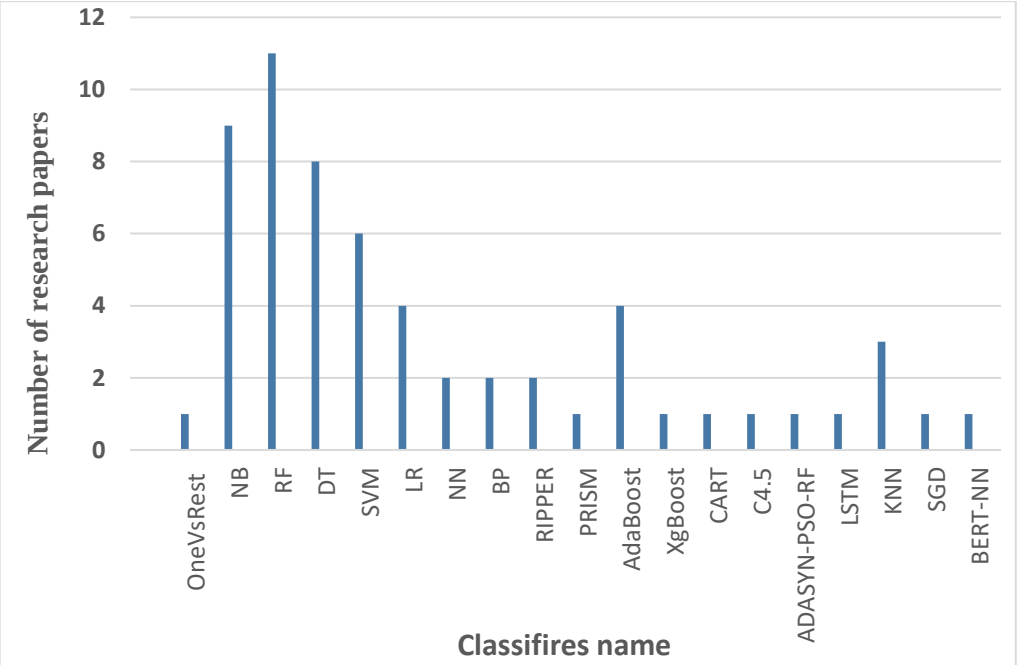

Figure 4: Classifier presence in several publications presented in this review from 2017 to 2022

Table 1: Comparison of machine learning-based anti-smishing

Reference	Approach	Dataset	Extracted feature	Feature selection	Classifier	Results	Limitation
[6]	SMS contents	——	Term frequency (TF)	——	NB	The system provides protection, accessibility, and dependability in the face of increasingly complex and malicious security risks by utilizing the machine learning method. It also protects against malicious activities such as personal information leakage and unauthorized charge payments.	There is no verification of the URL's legitimacy. There is no check for the presence of an email id in the message.
[7]	Heuristic	[25], [26], [27]	TF	correlation algorithm.	RF DT SVM AdaBoost	In terms of accuracy, the results are promising: 96.40%, 84.38%, 77.28%, and 93.24% for the	There was a problem with the model's upper limit on the number of features that

Table 1:

						English dataset and 90.33%, 89.75%, 89.08%, 90.51% for the non-English dataset for f-score, recall, and precision, respectively. Even after nearly half of the features were pruned, the accuracy in the English dataset was 96.16%.	could be added to the set. After feature selection, accuracy was lower than before feature selection. No check for the legitimacy of the URL
[8]	SMS contents	[25]	data mining	———	DT RIPPER PRISM.	In terms of TPR, RIPPER outperformed DT and PRISM, which showed 90.88% and 72.65%, respectively. The RIPPER had a TNR of 99.01%, while the DT and PRISM had 99.17% and 99.93%, respectively.	No check for the legitimacy of the URL
[9]	SMS contents	_____ __	——	——	NB	The system provides security against smishing risks	The blacklist URL was ineffective because the malicious URL was frequently updated.
[10]	SMS contents	[25]	N-gram	BPSO	RF ADASYN-RF ADASYN-PSO-RF	The best accuracy was 99.01% when one-sixth of the samples were used as testing data and five-sixths of the samples were used as training data. LIWC features and topic features improve performance by up to 98.13%	No check for the legitimacy of the URL

Table 1: continue

						for single-type features	
[4]	SMS contents	[25]	TF-IDF(term frequency-inverse document frequency)	————	OneVsRest	It provides more reliable security in terms of detection rate and false-positive results prevention.	No check for the legitimacy of the URL
[11]	Heuristic	[25], [26]	TF-IDF	———	SVM LR RF	SVM and RF classifiers achieve the highest F1 score, The precision of the classifiers SVM, RF, and LR was 88%, 88%, and 89%, respectively.	No check for the legitimacy of the URL
[12]		[25], [26]	TF	IG	SVM LR NN NB RF	It detects smishing with a TPR of 94.20%TPR, a TNR of 99.08%, and an accuracy of 98.74%. It is particularly effective at spotting zero-hour attacks.	The feature set was based on the text content of the message. No check for the legitimacy of the URL
[13]	SMS contents	[25], [26]	TF-IDF	———	NB RF DT	In the SMS Content Analyzer module. Using NB classifier showed 91.6%, 93%, 92%, 92% for accuracy, precision, recall, F1-score respectively. Overall accuracy after evaluating all four models showed 96.29% accuracy.	The authenticity of the application downloaded through the APK Detector module was not guaranteed
[14]	SMS contents	[25], [26]	TF	IG	NB NN LR	It detected spam messages with 0.949, 0.953, 0.985, 0.959, 0.294, and 0.985 for accuracy, roc recall,	The feature set is dependent on the message's text content, and it is not capable of

Table 1:

						precision, FPR and TPR respectively. smishing messages can be detected with 0.960, 0.958, 0.932, 0.994, 0.007, 0.932 for accuracy, recall, precision, FPR, TPR, respectively	detecting malicious applications. No check for the legitimacy of the URL
[15]	Heuristic	[25]	TF-IDF	Kendall rank correlation	RF DT SVM AdaBoost	When selecting all features AdaBoost was the best classifier result with 98.67%, 94.86%, 92.23%, and 97.75% for accuracy, F1-score, precision, and recall respectively. After applying correlation algorithms specifically, Kendall ranking, the results were 98.40%, 93.97%, 91.42%, and 96.49% for accuracy, F1-score, recall, and precision respectively.	No check for the legitimacy of the URL
[16]	Combination of SMS contents and URL behavior	[25], [26]	TF	———	BP RF NB DT	The RF achieved 97.85% accuracy, while the BPA achieved the highest accuracy of 97.93%. The NB also performed well, with an accuracy of 97.76%. DT achieved 96.48% accuracy.	The phone number and email address in a message were not checked for maliciousness.

Table 1: continue

						BPA and RF accuracy and recall were nearly identical, with values of 84% and 94%, respectively. The AUC (Area under the ROC Curve) score 0.988, 0.985, 0.983, 0.974 for BP, RF, NB and DT respectively	
[17]	SMS contents	[25]	TF-IDF and N-gram	ANOVA	XGBoost RF CART SVM AdaBoost	SVMs outperformed the other classifiers by achieving 98.39%, 98.37%, 99.79%, and 99.08% for accuracy, precision, recall, and F1-score respectively	No check for the legitimacy of the URL
[18]	SMS contents	[25]	TF	————	LSTM KNN SGD DT NB RF	LSTM achieved the best result with 95.11%, 94.88%, 91.07%, and 99.03% for accuracy, F1-score, recall, and precision respectively	No check for the legitimacy of the URL
[19]	Combination of SMS contents and URL behavior	[25] and set of Arabic messages	TF-IDF and word embedding	————	Bert And Fully Connected Neural Network (BERT-NN)	The model results were 99.63% in terms of accuracy, 9.72% precision, 97.48% recall, 98.1% F1-Score, 98.67%	The dataset was not very large which led to the prevention of detection of other types of smishing messages
[20]	SM S contents	labeled data set with 5000 data points [20]	TF-IDF	————	NB RF	The system achieved 90.59% accuracy and 72.09% F1-score for NB, and RF showed 98.15%	No check for the legitimacy of the URL

						accuracy and 92.57% F1-score.	
[5]	Combination of SMS contents and URL features	[25], [26]	TF	NN	DT NB NN	The NN showed 97.40% accuracy and 92.37%, and 97.91% for TPR and TNR respectively	Because the malicious URL was frequently updated, blacklisting it was not very useful.
[21]	SMS contents	[25]	TF	——	RIPPER C4.5	The number of correctly classified instances was 98.42% and 1.58 % in cases incorrectly labeled. C4.5 achieved a TPR of 0.995, an FPR of 0.084, and precision and recall of 0.987 and 0.995	No check for the legitimacy of the URL
[22]	Heuristic	[22]	——	——	——	The VirusTotal API had the highest detection rate of 99.27% with a response time of 12-15 seconds per query for the sensitive security application Furthermore, for the time-sensitive application The Safe-Browsing API has an 87% accuracy and a response time of 0.15ms	The system only checks the maliciousness of the URL without analyzing the SMS content.
[23]	SMS contents	Swahili text SMS [23]	TF TF-IDF	IG	(Multinomial NB) LR SVM KNN RF AdaBoost DT	The best performance achieved by RF was 99.86%	The results indicate that none of the models distinguished between classes perfectly. This occurred because false positive and

Table 1:

							false negative classifications are available. No check for the legitimacy of the URL
[24]	Combination of SMS contents and URL behavior	[25], [26] 121 SMS from URL dataset of 507195 unique entries.	TF-IDF	——	KNN RF ETC Voting	The proposed technique achieved 99.03% and 98.94% accuracy and precision respectively	The system trained phishing URLs without checking URL authenticity

4. Discussion

First, the user should recognize specific smishing words such as abbreviations in SMS and leet words in both SMS and URL, emotional phrases, misspelled words (such as the attackers used misspelled words in the message body or URL), shortcodes, and impersonality.
Second, installing protective applications from trusted source devices/phones because several attacks could be lanched without the user's knowledge by clicking on malicious links to download malware, which ends with harming the user's information.
Finally, it is important to check the permission of the applications before downloading them to determine whether those requests for access to SMS, contacts, camera, etc. are legitimate. Since attackers mostly use impersonal messages so they can be sent to the largest number of victims.

As mentioned in the previous section, the most commonly used classifier in SMS classification is RF. SMS content analysis is the most commonly used strategy in many approaches. Several studies use blacklists or whitelists to validate URLs, phone numbers, and email addresses. However, whitelisting cannot be used to detect smishing because it cannot recognize updated harmful features of URLs. Also, since blacklisting cannot detect zero-day phishing tactics, blacklists must be regularly updated.

5. Conclusions

In the era of advanced cybercrimes and attacks, the attackers intend to gather consumer information as quickly as possible. Therefore, the attackers send SMS messages to mobile phones. The small size of a mobile phone's display, phone users' lack of understanding of security programs, and open unknown source messages prevent the user from seeing the entire harmful link. The attacker sends a message to the user's phone that contains a malicious link that redirects them to a malicious website where they are asked to submit personal information. This type of cyber-attack is referred to as smishing.

Combating smishing messages necessitates user education. The key premise that emerges from this review is that different approaches can play an important role in detecting smishing. In addition, a comparison of various approaches for distinguishing smishing messages from genuine messages, as well as their results and limitations was provided. Recent research and studies indicate that combining URL behavior analysis and SMS content analysis with a large dataset is the best strategy for combating smishing . This will direct the researchers interested in developing more effective anti-smishing methods in the future.

References

[1] S. M. Hameed and M. B. Mohammed, "Spam Filtering Approach based on Weighted Version of Possibilistic c-Means," *Iraqi J. Sci*., vol. 58, no. 2C, pp. 1112–1127, 2017, doi: 10.24996/ijs. 2017.58.2c.15

[2] M. M. Hoobi, "Strong Triple Data Encryption Standard Algorithm using Nth Degree Truncated Polynomial Ring Unit," *Iraqi J. Sci.*, vol. 58, no. 3C, pp. 1760–1771, 2017, doi: 10.24996/ijs. 2017 .58.3c.19.

[3] E. Zhu, Y. Ju, Z. Chen, F. Liu and . X. Fang, "DTOF-ANN: An Artificial Neural Network phishing detection model based on Decision Tree and Optimal Features," *Applied Soft Computing Journal*, vol. 95, p. 106505, Oct 2020.

[4] S. Mishra and D. Soni, "A Content-Based Approach for Detecting Smishing in Mobile Environment," in *International Conference on Sustainable Computing in Science, Technology & Management (SUSCOM)*, pp.986–993, 2019, https://doi.org/10.2139/ssrn.3356256.

[5] S. Mishra and D. Soni, "Implementation of 'Smishing Detector': An Efficient Model for Smishing Detection Using Neural Network," *SN Computer Science*, vol. 3, no. 3, May 2022, DOI: 10.1007/s42979-022-01078-0.

[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," *Telecommun System*, vol. 66, no. 1, pp. 29-38, 2017.

[7] G. Sonowal and K. S. Kuppusamy, "SmiDCA: An Anti-Smishing Model with Machine Learning Approach," *The Computer Journal*, vol. 61, no. 8, pp. 1143-1157, Aug. 2018.

[8] A. K. Jain and B. Gupta, "Rule-Based Framework for Detection of Smishing Messages in Mobile Environment," *The 6th International Conference on Smart Computing and Communications.*, vol. 125, pp. 617-623, 2018.

[9] D. Goel and A. K. Jain, "Smishing-Classifier: A Novel Framework for Detection of Smishing Attack in Mobile environment," *In International conference on next generation computing technologies.Springer*, pp. 502–512, oct2017.

[10] T. Wu, K.-F. Zheng, C.-h. WU and X.-j. WANG, "SMS phishing detection using oversampling and feature optimization method," in *International Conference on Information, Electronics, and Communication Engineering*, Beijing, China, pp.235-245, Dec 2018.

[11] C. Balim and E. S. Gunal, "Automatic Detection of Smishing Attacks by Machine Learning Methods," in *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, Ankara, Turkey, pp. 1–3, Nov 2019.

[12] A. K. Jain and B. B. Gupta, "Feature Based Approach for Detection of Smishing Messages in the Mobile Environment," *Journal of Information Technology Research*, vol. 12, no. 2, pp. 17-35, April 2019.

[13] S. Mishra and . D. Soni, "Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis," *Future Generation Computer Systems-the International Journal of Science*, vol. 108, pp. 803-815, 2020.

[14] A. K. Jain, S. K. Yadav, N. Choudhary, "A novel approach to detect spam and smishing SMS using machine learning techniques," *Research Anthology on Securing Mobile and Applications*, vol. 12, no. 1, pp. 21–38, 2020.

[15] G. Sonowal, "Detecting Phishing SMS Based on Multiple Correlation Algorithms," *SN Computer Science*, vol. 1, no. 6, pp. 1-9, 2020.

[16] S. Mishra and . D. Soni, "DSmishSMS-A System to Detect Smishing SMS," *Neural Computing and Applications*, vol. 45, pp. 1-18, Jul. 2021.

[17] R. E. Ulfath, I. H. Sarker, M. J. M. Chowdhury, and M. Hammoudeh, "Detecting smishing attacks using feature extraction and classification techniques," Lect. Notes Data Eng. Commun. Technol., vol. 95, pp. 677–689, 2022, DOI: 10.1007/978-981-16-6636-0_51.

[18] S. S. Shravasti and M. Chavan, "Smishing detection: Using artificial intelligence," *International Journal for Research in Applied Science and Engineering Technology*, vol. 9, no. 8, p. 2218–2224, March 2021.

[19] A. Ghourabi, "SM-Detector: A security model based on BERT to detect SMiShing messages in mobile environments," Concurr. Comput. Pract. Exp., vol. 33, no. 24, pp. 1–15, 2021, DOI: 10.1002/cpe.6452.

[20] B. E. Boukari, A. Ravi and . M. Msah, "Machine Learning detection for SMiShing frauds," in *IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, pp 1–2, 2021, https://doi.org/10.1109/CCNC49032.2021.9369640,

[21] O. N. Akande, H. B. Akande, A. A. Kayode, A. A. Adeyinka, F. Olaiya, and G. Oluwadara, "Development of a Real Time Smishing Detection Mobile Application using Rule Based Techniques," *Procedia Computer Science*, vol. 195, pp. 95-102, 2022.

[22] C. Thorpe and P. Phadke, "Analysis of API Driven Application to Detect Smishing Attacks" in *Conference: 20th European Conference on Cyber Warfare and Security (ECCWS)*, pp. 1–12, 2021, http:// DOI:10.34190/EWS.21.051.

[23] I. S. Mambina, J. D. Ndibwile, and K. F. Michael, "Classifying Swahili Smishing Attacks for Mobile Money Users: A Machine-Learning Approach," *IEEE Access*, vol. 10, August, pp. 83061–83074, 2022, DOI: 10.1109/ACCESS.2022.3196464.

[24] A. K. Jain, B. B. Gupta, and K. Kaur, "A content and URL analysis - based efficient approach to detect smishing SMS in intelligent systems," July, pp. 1–25, 2022, DOI: 10.1002/int.23035.

[25] T. A. Almeida, J. M. G. Hidalgo, and A. Yamakami, "Contributions to the study of SMS spam filtering: New collection and results," *DocEng 2011 - Proc. 2011 ACM Symp. Doc. Eng.*, pp. 259–262, 2011, DOI: 10.1145/2034691.203474.

[26] Pinterest,"smishing data set",20 Nov 2018 [Online]. Available: https://in.pinterest.com/seceduau/smishing-dataset/?lp=true.[Accecced]15 jan 2021.

[27] K. Yadav, P. Kumaraguru, A. Goyal, A. Gupta, and V. Naik, "SMSAssassin: Crowdsourcing driven mobile-based system for SMS spam filtering," *HotMobile 2011 12th Work. Mob. Comput. Syst. Appl.*, March, pp. 1–6, 2011, DOI: 10.1145/2184489.21844