iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VIII **Month of publication:** August 2021

DOI: https://doi.org/10.22214/ijraset.2021.37737

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

Smishing Detection: Using Artificial Intelligence

Samyak Sadanand Shravasti[1], Manik Chavan[2]
[1, 2]*Department of Computer Science and Engineering, Walchand College of Engineering (An Autonomous Institute), Sangli, India*

Abstract: Phishing occurs when people's personal information is stolen via email, phone, or text communications. In Smishing Short Message Service (SMS) is used for cyber-attacks, Smishing is a type of theft of sensitive information. People are more likely to give personal information such as account details and passwords when they receive SMS messages. This data could be used to steal money or personal information from a person or a company. As a result, Smishing is a critical issue to consider. The proposed model uses an Artificial Intelligence to detect smishing. Analysing a SMS and successfully detecting Smishing is possible. Finally, we evaluate and analyse our proposed model to show its efficacy.
Keywords: Phishing, Smishing, Artificial Intelligence, LSTM, RNN

I. INTRODUCTION

Phishing is a cybercrime where a fraudster contacts people by email, phone or instant message by pretending a genuine entity to collect delicate information from people. That information may contain personal data, banking details and passwords. This data can be used for identity fraud and monetary fraud [1].

Smishing is subset of phishing. In smishing text message is used to perform cyber-attack. Word "Smishing" is a combination of two words "Phishing" and "Short Messaging Service (SMS)". In Smishing fraudster uses SMS as a medium of attack. Smishing message contains words that lures person in deceiving themself to become victim of cyber-attack. Smishing message may contain Uniform Resource Locator (URL), Electronic Mail (Email) or phone number. By using any of this fraudster can steal persons credentials information. The Fig. 1 shows the example of smishing message.

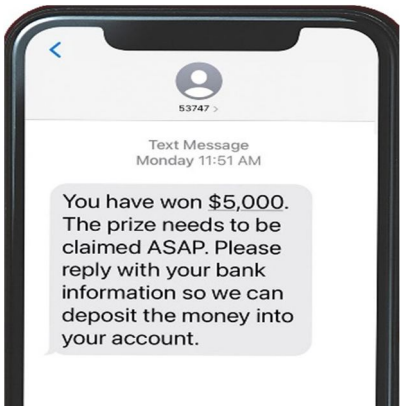


Fig. 1 Smishing Example

Anti-Phishing Working Group (APWG) is an association of not-for-profit organisations deals with the growing problem of phishing, crimeware, and email spoofing, which results into identity theft and frauds. Through 2020, the number of phishing scams identified by APWG, and its members increased by a factor of two [2]. The increasing threat of phishing attack is major concern.

A. *Techniques* used to detect Smishing

Following are the smishing detection techniques

1) *Filtering based on content:* In this technique message is tested with suspicious phone numbers, email IDs, URLs and keywords. In this technique content of message is analysed. By analysing content smishing is detected.
2) *Whitelisting:* In White-listing, saved trusted URLs called white-list can be utilized for to identify real sites. It makes easy for the classification method by avoiding lookup for real sites with harmful features. Whitelisting should be used in combination with other techniques because it cannot recognize the malicious URLs.
3) *Blacklisting:* In this method, reputable sites maintain a list of suspicious sites and URL's that can be used to identify fraudulent sites. This approach utilized by different intuitive programs. As blacklisting can't recognize phishing which are not recorded in blacklist. The blacklist should be refreshed routinely. Blacklisting cannot identify new phishing adequately.

4) *Heuristic methods:* In heuristic-based approach, Machine learning based classification is used to identify smishing message. In this approach dataset containing both legitimate and smishing SMS is used to perform classification. Result of this method is highly accurate but there is a possibility of result being false positive.
5) *URL Based methods:* In URL Based methods, URL is extracted from text message. This URL further inspected for malicious websites. if malicious URL is identified then it is smishing message. This method limits to only URL content of message.

II. LITERATURE SURVEY

In this study [4], the author proposed a system which analyses SMS contents to detect improper sentences which determines the possibility of phishing attacks. This system is different compared to previous work because it focuses on the natural language contents of message. It performs semantic analysis of the content to identify phishing. It utilizes question-answering and verb-object semantic information. Because it is based on content analysis, it makes this approach capable of detecting scams using non-email means, instant text message software and on call attacks which first converted to text by using a speech-to-text software then process text to determine phishing. In this study [5], the author proposed system which uses machine learning for identifying smishing. There are three stages in this model which are prepossessing, feature extraction and classification. Prepossessing involves Tokenization, removal of punctuation's, obtaining root or stem of words. after that in feature extraction following features are extracted form message which are Term, URL, Phone number, Email, Character count, money, to classify message into legitimate and smishing. Author has used Random Forest, Support Vector Machine and Logistic Regression Classifiers.

In this study [6], Author uses a rule-based method to distinguish whether message is legitimate or smishing. Set of rules are used for classifying content. There are nine rules in this system, which are used to classify message into legitimate and smishing. Rules are as follows Presence of URL, math symbol, currency sign, mobile number, suspicious keywords, message length greater than 150, self-answering type and Visual morphemes. This system utilizes classification methods to train these nine rules. Classifiers are Decision Tree, RIPPER, PRISM. By applying these classification methods Smishing messages are detected.

In this study [7], the author proposed "S-Detector" which is an anti-smishing model. For identifying and filtering legitimate and smishing messages, this system uses a combination of URL and content-based techniques. This system has four parts, which are SMS analyser, SMS monitor, Database, and SMS determinant. URL and smishing keywords are identified from message content. For classification it uses Naive Bayesian classifier. If URL is found in message, then it is further checked for auto download of an android app. This system categorizes message into smishing if it contains URL which can download android app, or it contains high amount of smishing keywords. This study [8] proposes a real-time network based on community for collecting malicious threat intelligence from anonymized communication records sent by smartphone users. The information is then updated to users in real-time. This system also provides Android application's Realtime analysis that are triggered by URLs in SMS to be installed. It also has the distinct capability of comparing downloaded software to known viruses at Realtime. It is done through their hash-valued n-gram search index, which makes addition to traditional databases and takes advantage of features currently available in commercial database systems. This paper [9], To detect Phishing through email, new classification model is proposed which is THEMIS, which is based on Recurrent Convolution Neural Network (RCNN). It efficiently detects phishing. To detect Phishing, this system examines the email header and body. The accuracy of this model approaches 99.848%, which is higher than that of other neural networks, according to experimental results.

III.METHODOLOGY

A. *Dataset*

In this work SMS Spam Collection Data set [10] is used to analyse, evaluate messages and detect smishing. This data set contains 5572 SMS records. It has two attributes Category and Message. There are 4825 ham messages that is legitimate messages and 747 spam messages that is smishing messages. Fig. 2 shows schema of data set.

	Category	Message
0	ham	Go until jurong point, crazy.. Available only ...
1	ham	Ok lar... Joking wif u oni...
2	spam	Free entry in 2 a wkly comp to win FA Cup fina...
3	ham	U dun say so early hor... U c already then say...
4	ham	Nah I don't think he goes to usf, he lives aro...
...	...	...
5567	spam	This is the 2nd time we have tried 2 contact u...
5568	ham	Will ì_ b going to esplanade fr home?
5569	ham	Pity, * was in mood for that. So...any other s...
5570	ham	The guy did some bitching but I acted like i'd...
5571	ham	Rofl. Its true to its name

5572 rows × 2 columns

Figure 2 SMS Spam Collection Data set

B. System Design

In this section, the natural language pre-processing and deep learning-based methodology is discussed. Fig. 3 Illustrates the System design of the proposed method.

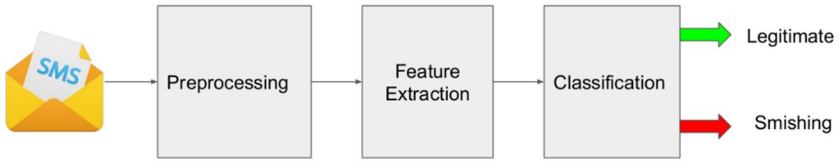


Fig. 3 System Design of Smishing Detection System

C. Pre-processing

In Pre-processing SMS form scam dataset is pre-processed using following natural language pre-processing techniques.

1) *Tokenization: Splitting the sentence into words.*
2) *Convert text to lowercase.*
3) *Remove Punctuation.*
4) *Remove English stop words.*
5) *Strip whitespaces.*
6) *Stemming and Lemmatization: Generate the root form of the words.*

D. Feature Extraction

After SMS data is pre-processed, Features are extracted from it and used for analysis. In this stage following features are extracted,

1) *Term Feature*
2) *URLs*
3) *Email address*
4) *Mobile number*
5) *Character count*
6) *Currency character*

All extracted features are further analysed by plotting different charts.

E. Classification

The next stage is classification, which involves training and testing scam SMS data on various machine learning and deep learning models. For classification models used are Long Short-Term Memory Recurrent Model (LSTM), KNeighbors, Stochastic Gradient Descent (SGD), Decision Tree, Naive Bayes and Random Forest Classifiers. From these classifiers LSTM gives maximum accuracy hence it is used in prototype to identify smishing and legitimate messages.

F. Evaluation of F-Score Measures:

In this work, F-score measure is used to evaluate the performance of Smishing Detection System. Fig. 4 show confusion matrix which is used to calculate Accuracy, Recall, Precision and F_1-Score. Terminologies used in Fig. 4 are True positive (TP), False Negative (FN), False Positive (FP) and True negative (TN). Formulas for are given bellow,

		Predicted Class	
		Positive	Negative
Actual Class	Positive	TP	FN
	Negative	FP	TN

Fig. 4 Confusion Matrix

$$Recall = \frac{TP}{TP + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$F_1 = 2 \times \frac{precision \times recall}{precision + recall}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

IV. OUR WORK

Nowadays use of smartphones and social media have been increased Drastically. We can interact with people with the simple message. We are leveraging smartphones by consuming services like mobile banking, mobile wallet, internet banking because of this we are at ease of doing our financial tasks by just performing few clicks on the smartphone. Although this is very useful to us, but some people are misusing this medium of communication by Phishing people through SMS which is called Smishing. Smishing Attacker convinces a victim to perform actions which will result in financial loss of a victim. To prevent Smishing, we are proposing a Smishing Detection System based on Artificial Intelligence. Long Short-Term Memory Recurrent Neural Network is used to detect Smishing.

V. RESULT AND DISCUSSION

Almost Everyone uses smartphones these days, Because of this Phishing attacks are increasing. Smartphones are widely used for communication and financial services. Scammers are targeting smartphone user through smishing messages. There is need of such system which help people from being scammed. Artificial Intelligence can enhance smartphone security by analyzing messages received by users and provide vulnerability alerts to users and prevent smishing. In this work we have studied different smishing detection systems and proposed system which uses Artificial Intelligence to help people in distinguishing cyber threat like smishing from normal messages. As mentioned in methodology section, First SMS is preprocessed. Then features are extracted from SMS to analyze these features. Features are Term Feature, URL'S, Email address, Mobile number, character count and currency character. After that extracted feature are provided to classification algorithm. Classifier classifies message as legitimate or smishing. The data set was not balanced, it was showing wrong results, First Data set is balanced then used for further analysis.

A. Message Character Count

As Fig.5 shows character count of ham message is less than legitimate message. Smishing messages are shorter than legitimate messages.

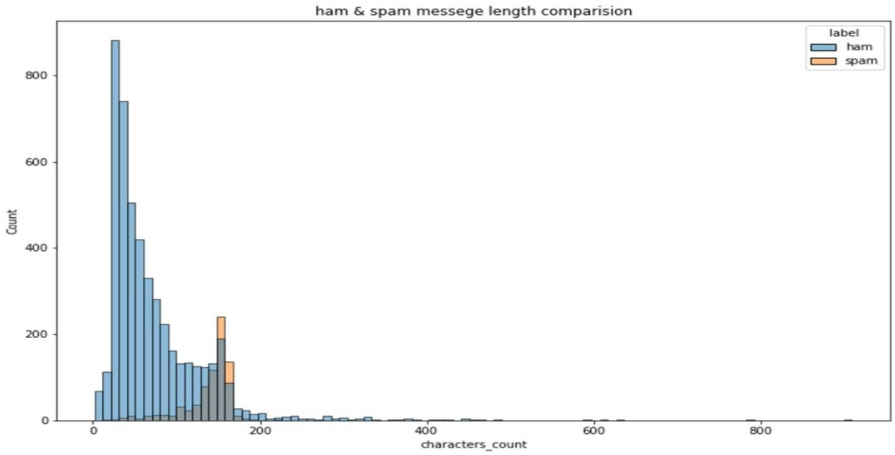


Fig. 5 Message Character Count

B. Money Character Count

As Fig.6 shows most of spam messages contains money characters but most of legitimate messages does not contains money characters.

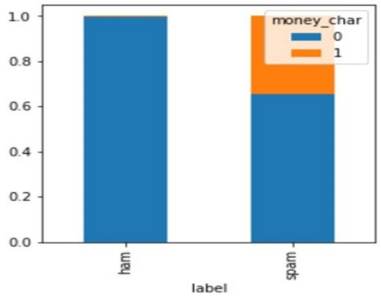


Fig. 6 Money Character Count

C. Message URL's

As Fig.7 shows most of spam messages contains URLS's but most of legitimate messages does not contains URL's.

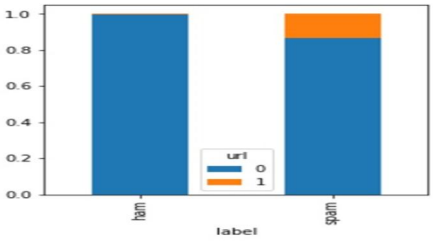


Fig. 7 Message URL's

D. Prototype of Smishing Detection System

Prototype of Smishing Detection System is developed using Flask framework. Python is used for backend and bootstrap framework is used to design frontend.

1) Input No. 1: First Legitimate message is given as input to the system as shown in Fig. 8.

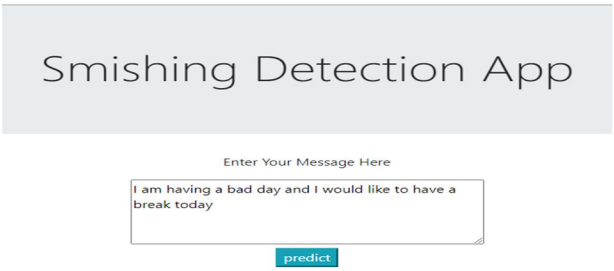


Fig. 8 Input No. 1

2) Output No. 1: Then System detects input message as legitimate message and gives the output as shown in Fig. 9.

Fig. 9 Output No. 1

3) Input No. 2: Secondly spam message is given as input to the system as shown in Fig. 10.

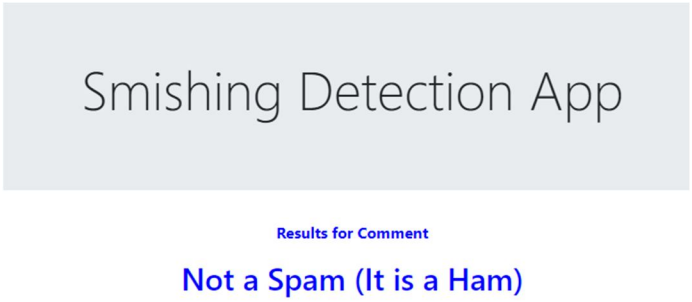


Fig. 10 Input No. 2

4) Output No. 2: System detects input message as Smishing message and gives the output as shown in Fig. 11.

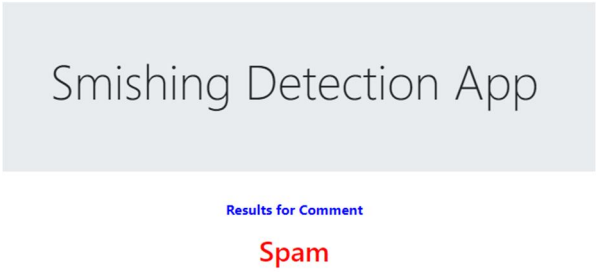


Fig. 11 Output No. 2

E. F1-Score Table

The proposed system is tested on different classification models. Used classification models are Long Short-Term Memory Recurrent Model (LSTM), KNeighbors, Stochastic Gradient Descent (SGD), Decision Tree, Naive Bayes and Random Forest Classifier. Table 1 shows the F1-Score results of the mentioned classifiers. LSTM scores higher than other classifiers. LSTM score 0.9488 and accuracy of model is 95.11%.

TABLE I
F1-SCORE

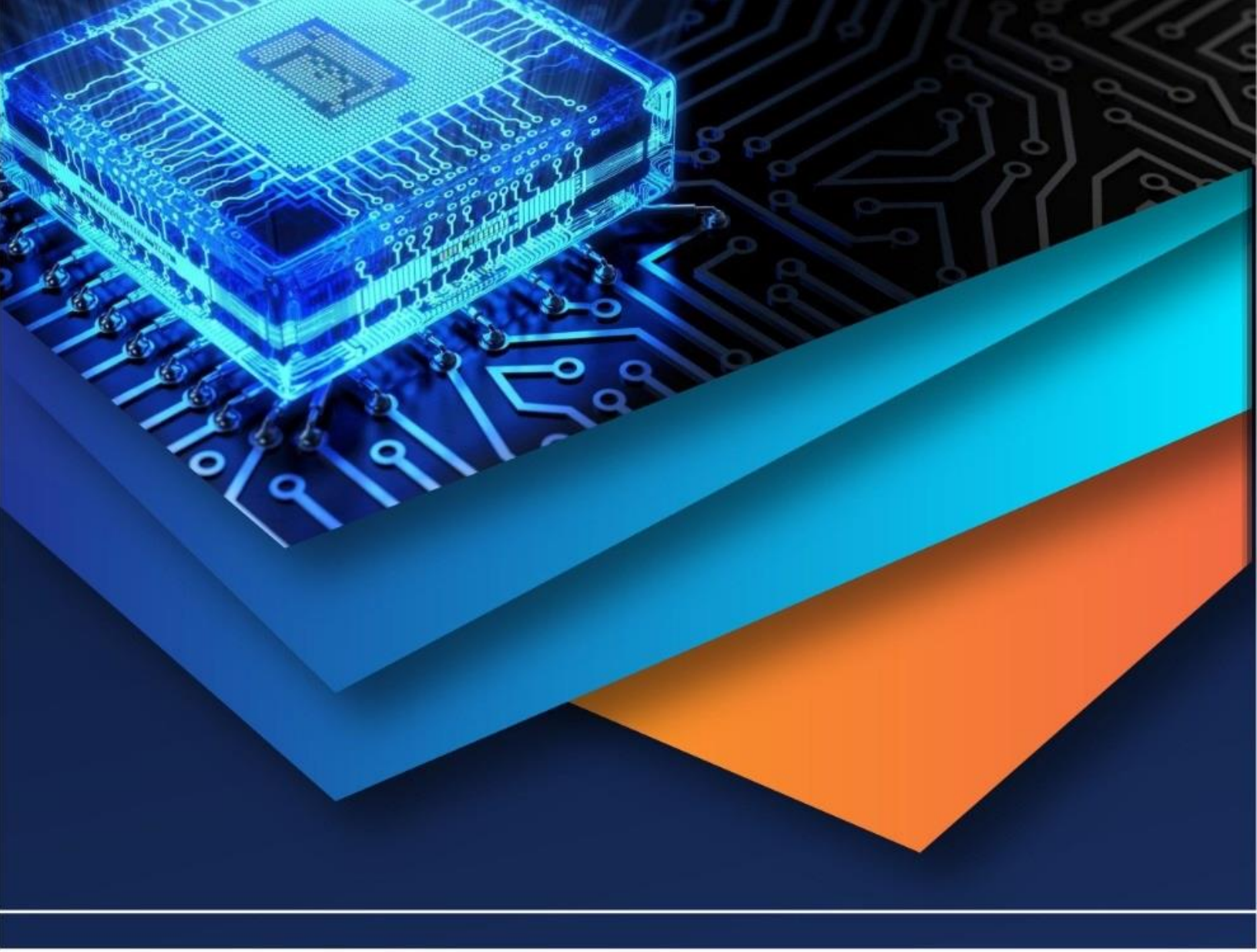
Classifier	Precision	Recall	F1-Score
KNeighbour	0.8279	0.8211	0.8245
SGD	0.6644	0.7886	0.7212
Naive Bayes	0.8286	0.7073	0.7632
Decision Tree	0.7913	0.7398	0.7647
Random Forest	0.8203	0.8537	0.8367
LSTM	0.9903	0.9107	0.9488

VI. CONCLUSION

As the number of smartphone users increasing, Cyber attackers are targeting smartphone users. The proposed work uses the deep learning-based model to identify a Smishing attack and protect smartphone users from being exploited by cyber attackers. This work has trained and tested various classification models and found that Long Short-Term Memory Recurrent Neural Network gives maximum accuracy out of others. The proposed system identifies the message is smishing or legitimate based on the content of the message. The proposed model provides 95.11% accuracy.

REFERENCES

[1] "What Is Phishing?" Accessed on: Feb. 10, 2021. [Online]. Available: https://www.phishing.org/what-is-phishing
[2] "Phishing Activity Trends Report 4th Quarter 2020," Accessed on: Feb. 10, 2021. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf
[3] Mishra, S., & Soni, D. (2019). SMS Phishing and Mitigation Approaches. *2019 12th International Conference on Contemporary Computing, IC3 2019*, 1–5. https://doi.org/10.1109/IC3.2019.8844920
[4] Kim, M., Song, C., Kim, H., Park, D., Kwon, Y., Namkung, E., Harris, I. G., & Carlsson, M. (2019). Scam detection assistant: Automated protection from scammers. *2019 1st International Conference on Societal Automation, SA 2019*, 1–8. https://doi.org/10.1109/SA47457.2019.8938036
[5] C. Balim and E. S. Gunal, "Automatic Detection of Smishing Attacks by Machine Learning Methods," *1st International Informatics and Software Engineering Conference (UBMYK), Ankara, Turkey, 2019* pp. 1-3, doi: 10.1109/UBMYK48245.2019.8965429.
[6] A.K. jain and B.B. Gupta, "Rule-based framework for detection of smishing messages in mobile environment," *Procedia Computer Science, vol. 125, 2018* pp. 617-623.
[7] 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. Syst., 2007* vol. 66, pp. 1-10.
[8] K. Lee, W. Park, K. Cho and W. Ryu, "RealCatch: A community-based real-time platform for financial fraud protection on smartphones," *International Conference on Information and Communication Technology Convergence (ICTC), Busan, 2014* pp. 362-366, doi: 10.1109/ICTC.2014.6983155.
[9] Y. Fang, C. Zhang, C. Huang, L. Liu and Y. Yang, "Phishing Email Detection Using Improved RCNN Model With Multilevel Vectors and Attention Mechanism," *in IEEE Access, vol. 7* pp. 56329-56340, 2019, doi: 10.1109/ACCESS.2019.2913705.
[10] "SMS Spam Collection Data Set," Accessed on: Feb. 10, 2021. [Online]. Available: https://archive.ics.uci.edu/ml/datasets/sms+spam+collection



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY