DOI: https://doi.org/10.57233/ijsgs.v11i3.920 ISSNp: 2488-9229: ISSNe: 3027-1118

IJSGS FUGUSAU VOL. 11(3) WEBSITE: https://fugus-ijsgs.com.ng

INTERNATIONAL JOURNAL OF SCIENCE FOR GLOBAL USTAINABILITY
(A PUBLICATION OF FACULTY OF SCIENCE, FEDERAL UNIVERSITY GUSAU, NIGERIA)

A Deep Learning Approach to Smishing Detection in Mobile Apps Using Convolutional Neural Network and Long ShortTerm Memory

***[1]Ogah Muhammad Usman, [2] Tahir Abdulhakim [3] Ayinla Munirat Tope**

[1]Department of Computer Science, Nasarawa State University Keffi, Nasarawa State, Nigeria
[2]Department of Computer Science, Nasarawa State University Keffi, Nasarawa State, Nigeria
[3]Department of Computer Science, Nasarawa State University Keffi, Nasarawa State, Nigeria
Keffi, Nasarawa State.

***Corresponding Author's Email Address**:mohammedogah@gmail.com, abdullahitahir@nsuk.edu.ng, ayinlamunirat@gmail.com

Received on: August, 2025 **Revised and Accepted on:** September, 2025 **Published on:** October, 2025

ABSTRACT

Smishing, or SMS phishing, poses a significant cybersecurity threat to smartphone users. These attacks exploit the brevity and symbolic nature of SMS messages, making detection challenging. Existing methods, such as DSmishSMS, employ traditional machine learning techniques but require further enhancement. To address this rising and concerning issue, this thesis offers a model for an improved detection. The experiment demonstrate that the developed CNN model outperformed traditional algorithms, achieving an accuracy of 98.97% which is better than the 97.93% from the benchmark paper. By integrating deep learning techniques, this contributes to safeguarding users from fraudulent smishing attack.

Keywords: Smishing Detection, Deep learning, Mobile security, LSTM, CNN, Phishing.

I.0 INTRODUCTION

Phishing is a systematic type of scamming in which thieves pretend to be legitimate web pages with the aim to illegally obtain sensitive data from people and companies over the globe (International et al., 2021). Smisihing, also known as SMS phishing, is an attack when a hacker sends an encrypted text to a user that contains links to malicious websites, programs, or interfaces that ask for the user's credentials, or it provides the perpetrator's phone number or email address. Using these user interfaces, users divulge important information such as their payment card number, login credentials, and user ID. By means of this attack, perpetrators obtain private customer information, such as contact details, images, etc., in addition to financial gain (Mishra and Soni, 2020).

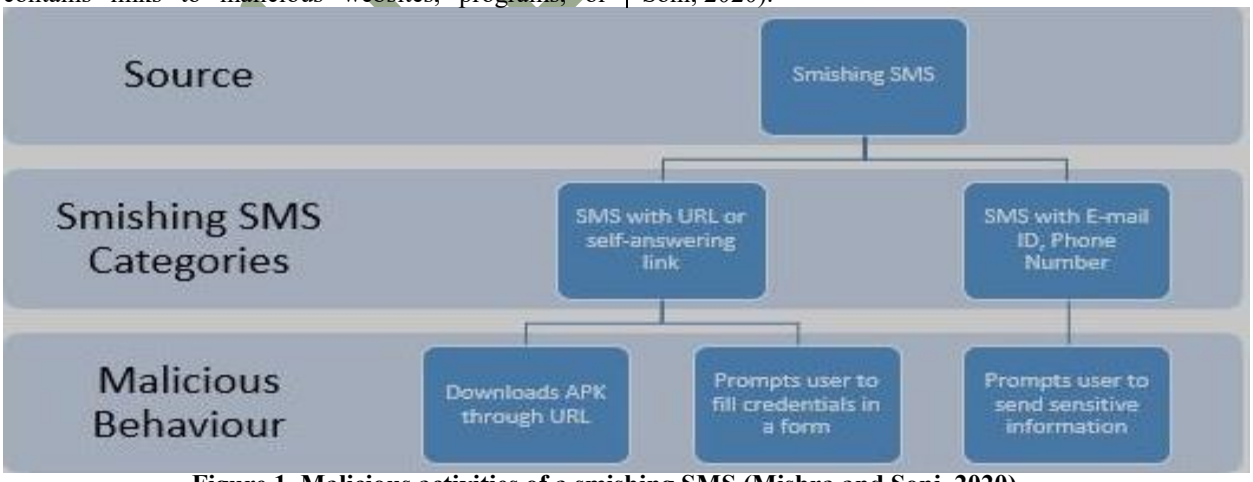


Figure 1. Malicious activities of a smishing SMS (Mishra and Soni, 2020)

DOI: XXXXXXXXXXXXXXXXX ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOLXXX WEBSITE: https://fugus-ijsgs.com.ng

A perpetrator who uses text message to targeted victims is known as a smisher. Telephone the number or transmit the data they provided to the email address that was included in the message. A sample of a counterfeiting telegram is shown in Figure 1 (Mishra and Soni, 2020). According to recent statistics on text message branding, 65% of people worldwide are able to converse using Short Message Service (SMS). By the end of 2025, researchers predict the above proportion will rise to 78% of the world's people (Fachkha, 2023). For instance, according to Wahsheh and Al-zahrani (2022), 76% of managers would rather use SMS as sirens for their required encounters.

1.2 Statement of Problem

The prevalence of Smishing (SMS phishing) attacks targeting smartphone users poses a significant cybersecurity threat due to the difficulty in detecting such fraudulent activities. Current detection methods face challenges stemming from the brevity and symbolic nature of SMS messages, the use of abbreviations and acronyms, and the sophisticated impersonation of legitimate brands by attackers (Mishra and Soni, 2021). Although systems like DSmishSMS have been developed to address these challenges using machine learning techniques such as Backpropagation algorithm, Naive Bayes algorithm and content analysis, there remains a need for further research to enhance the effectiveness and efficiency of smishing detection. Specifically, there is a gap in understanding how to improve detection accuracy by better extracting and analyzing relevant information from SMS messages, such as identifying disguised Uniform Resource Locators (URLs) and distinguishing legitimate brands from fraudulent ones. Therefore, this study aim to contribute to the advancement of smishing detection systems by using deep learning methodologies and technologies to detect smishing attacks targeting smartphone users.

1.3 Literature Review

Phishing is one of the most effective and well-known cyber threats, leading to millions of compromised credentials and contributing to 90% of data breaches (Aljofey, *etal.,* 2020). Phishing scams are becoming increasingly more deceptive with sophisticated attacks that are able to manipulate end-users through, for instance, spoofed websites, targeted emails, and fake phone calls (Wahsheh and Al-zahrani, 2022). Figure. 2. shows the examples of Smishing SMS.

(a) Smishing using URL (b) Smishing using Phone Number (c) Smishing using the Email ID

Figure 2. Examples of Smishing SMS (Mishra and Soni, 2020).

In recent years, several researchers have proposed solutions to identify SMS phising. They have employed smishing or legitimate methods . Other researchers have tried other classifiers, such as Random Forest and AdaBoost (Mishra and Soni, 2020) or even a rule-based classification (Wahsheh and Al-zahrani, 2022). An anti-phishing approach called as MobiFish was proposed by (Wu *et al.*, 2024). An enhanced security model for detecting Smishing attack called S-Detector is developed by (Woong *et al.*, 2024).

.

2.0 METHODOLOGY

Python TensorFlow environment was used to build and train the CNN model. Based on the developed model

DOI: XXXXXXXXXXXXXXXXX ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOLXXX WEBSITE: https://fugus-ijsgs.com.ng

.In Figure 3 the research approach is presented and Figure 4 presents the architecture of the proposed model.

This study adopted two deep learning algorithms Convolutional and Long Short Term Neural Networks with an optimizer enhancement technique which will enhance the models accuracy by reducing the error rate. These methods have been applied in previous similar situation of spam text classification and are proven to have solved similar problems with good result.

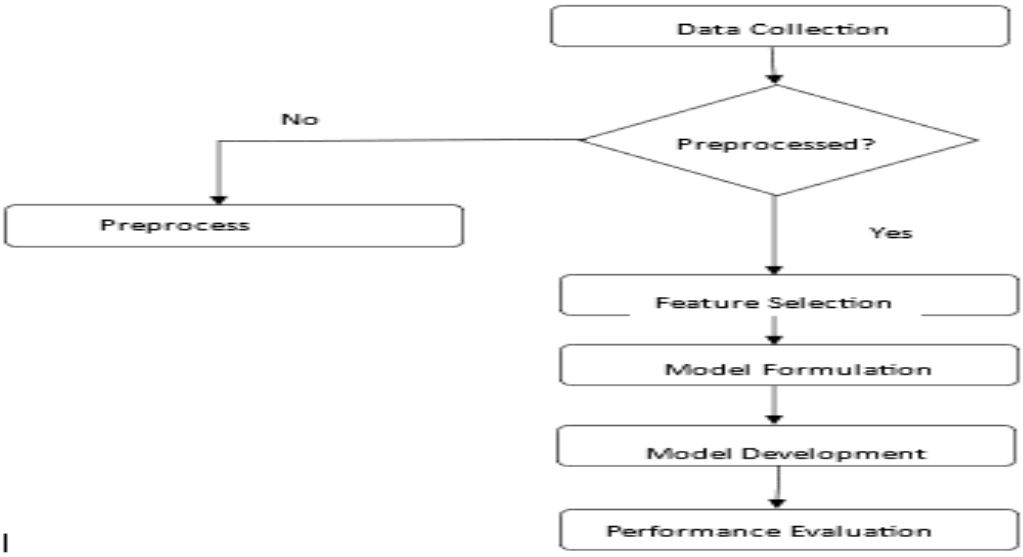
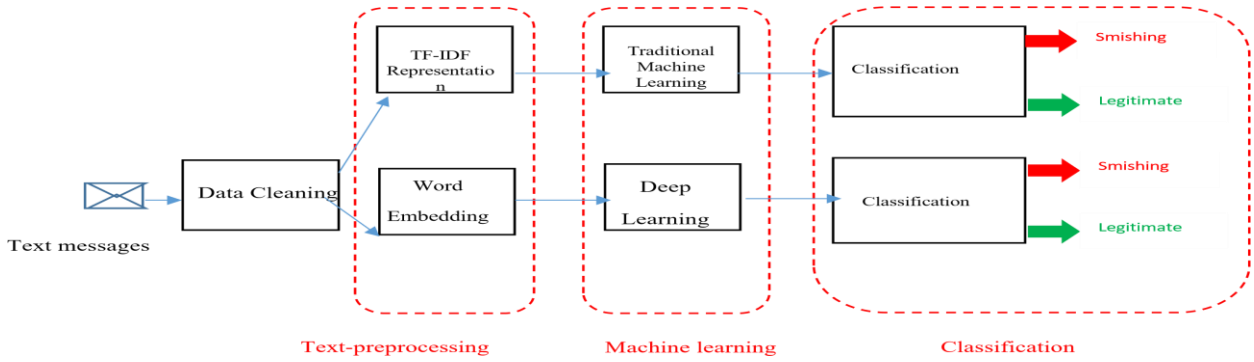


Figure 3. Research Approach Flowchart of The Model

In study, the purpose of word embedding is to prepare the textual data for the deep learning model. Figure 4 describes the steps performed to accomplish the word embedding process.

Figure 4. Word embedding process



DOI: XXXXXXXXXXXXXXXXX ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOLXXX WEBSITE: https://fugus-ijsgs.com.ng

Figure 5. Architecture of the smishing detection model

Algorithm 3: Enhanced Smishing Detection

Inputs: SMS (text message)
Outputs: Classification_Result (Smishing or Legitimate)
Status: Processing

```
1: Start
2: while Incoming_SMS.moveToNext do
3: Tokenize Incoming_SMS using Tokenizer_Function
4: for each token in Tokenized_SMS do
5:     if token matches Phone_Pattern then
6:       Set Classification_Result to Smishing
7:       Exit loop
8:     else if token matches URL_Pattern then
9:       Perform Domain_Check on URL_Token
10:      if Domain_Check is suspicious then
11:        Set Classification_Result to Smishing
12:        Exit loop
13       end if
14       else if token matches Email_Pattern then
15       Perform Email_Validation on Email_Token
16       if Email_Validation fails then
17       Set Classification_Result to Smishing
18       Exit loop
19       if Classification_Result is not set then
20       Set Classification_Result to Legitimate
21       end if
```

Algorithm 4: CNN-based Smishing Classification

Inputs: Tokenized_SMS (list of tokens)
Outputs: Classification_Result (Smishing or Legitimate)

```
1: Start
2: Load pre-trained word embeddings (e.g., GloVe or FastText)
3: Initialize CNN model architecture
4: Add convolutional layers with appropriate filters and activation functions
5: Add pooling layers (e.g., max-pooling)
6: Optionally, add recurrent layers (e.g., LSTM)
7: if Validation_Accuracy meets desired threshold then
8:         Set Classification_Result to Legitimate
9: else
10:        Set Classification_Result to Smishing
11: end if
12: End Algorithm
```

Figure 6 shows the app environment

DOI: XXXXXXXXXXXXXXXXX ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOLXXX WEBSITE: https://fugus-ijsgs.com.ng

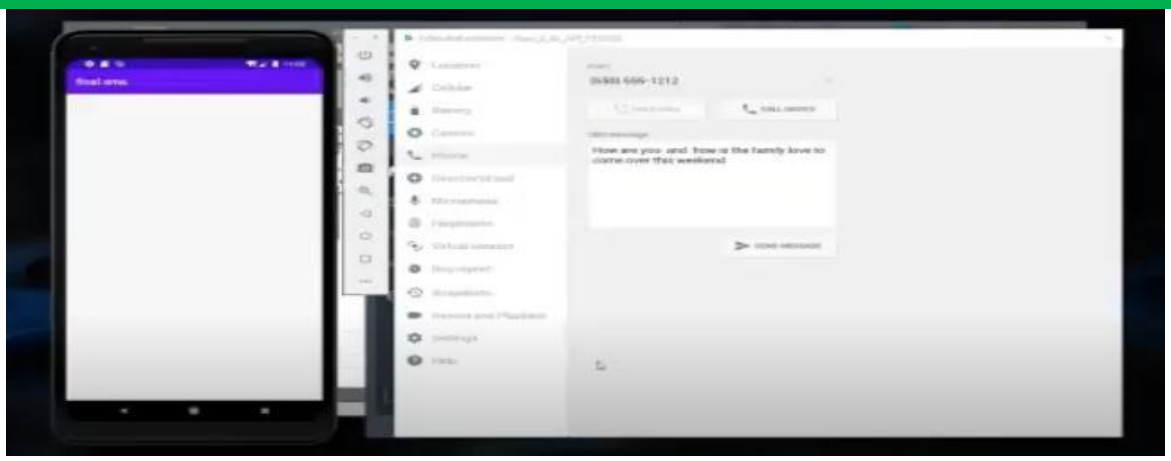
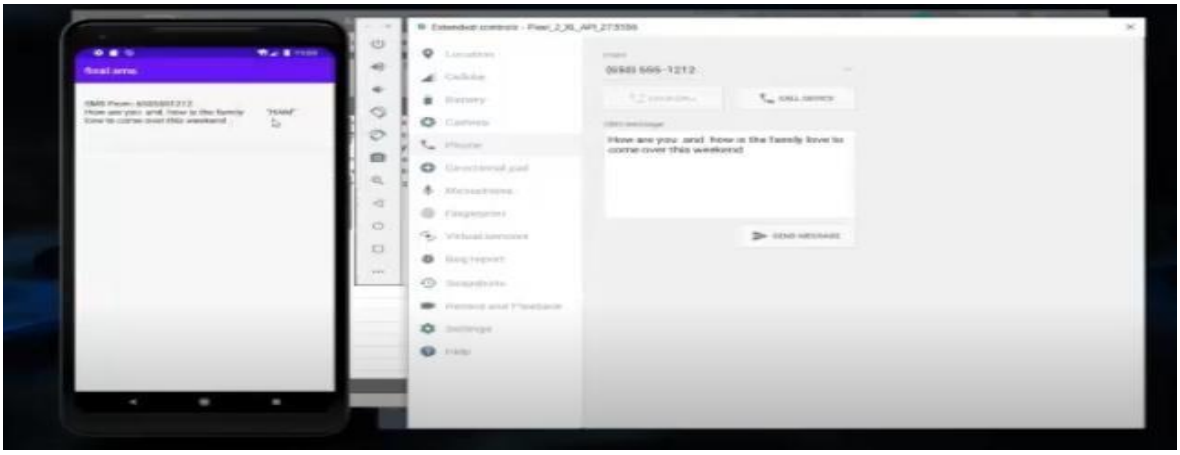


Figure 6. Mobile application environment

The right pane is the Android Studio background where sms messages are sent to the emulator on the left panel.The figure 6 shows a Dashboard containing some selected sms messages labeled as either smishing or legitimate from the dataset. This will be sent to the Android studio background for classification on the emulator

.



Figure

7. Dashboard of some selected SMS messages

Based on the selected sms messages the emulator will detect the sms messages

We have evaluated our approach using three machine learning algorithms, namely Decision Tree, Neural Network, and Naive Bayes. The detection results of each algorithm based on the feature values have been recorded.

3.0 RESULTS AND DISCUSSION

DOI: XXXXXXXXXXXXXXXXX ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOLXXX WEBSITE: https://fugus-ijsgs.com.ng

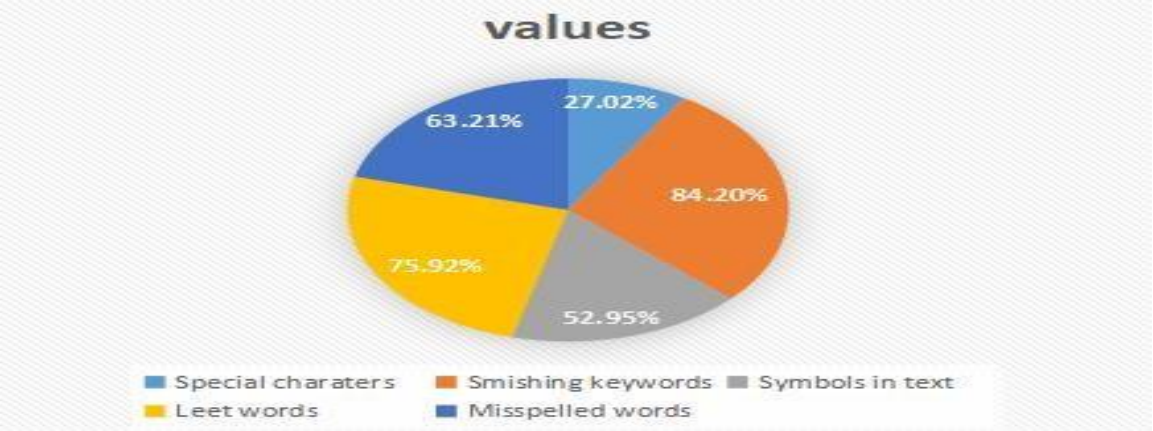


Figure 8. Frequency of each heuristic analyzed

The detection result of each algorithm is shown in Figure. 9. It shows that the Decision Tree Algorithm (DT) gave a decent accuracy of 97.85%, while Long Short

Term Memory (LSTM) gave an accuracy of 98.0, the Convolutional Neural Network Algorithm (CNN) gave an impressive performance 98.97%. The Naıve Bayes algorithm (NB) also presented a good performance with an accuracy of 97.76%. The precision and recall of CNN and DT are almost the same with a value of 94% and 84%, respectively.

Figure 9. Performance of Algorithms on our model

The sigmoid activation function was also tried for CNN, but we have achieved the best accuracy using ReLU Function for the CNN implementation of our system. Different values of learning rate were tested ranging from 0.1 to 1.0. The resultant graph and response to the error rate are depicted in Figure 9 shows that the error rate is rising in response to an increase in the learning rate.

Figure 10. Behavior of error to change in learning rate

DOI: XXXXXXXXXXXXXXXXX ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOLXXX WEBSITE: https://fugus-ijsgs.com.ng

Therefore, CNN has shown the best performance with an accuracy of 98.97% and execution time of 20.32 s.

The evaluation of the result of the model is depicted in Table 4. showing the four metrics of evaluation.

Table 4. Evaluation Results of the model

Algorithms	Accuracy	Precision	Recall	F1-score
Convolutional Neural Network (CNN)	98.97%	84%	94%	92%
Long Short Term Memory(LSTM)	98.00%	83%	92%	90%
Decision Tree	97.85%	82%	93%	78%
Naive Bayes	97.76%	67%	72%	86%
Neural Network	96.78	75%	69%	70%

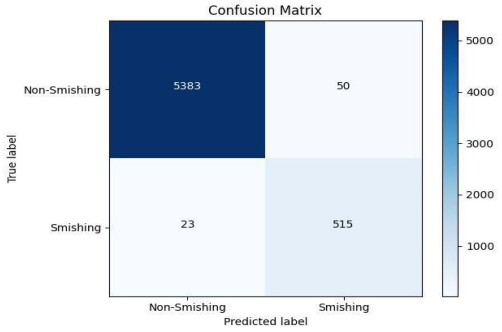


Figure 11: **A heat map showing the confusion matrix**

Figure 11 and figure 12 shows the confusion matrix and comparision with baseline paper . Therefore, CNN has gives an impressive accuracy of 98.97% with execution time of 20.32s.

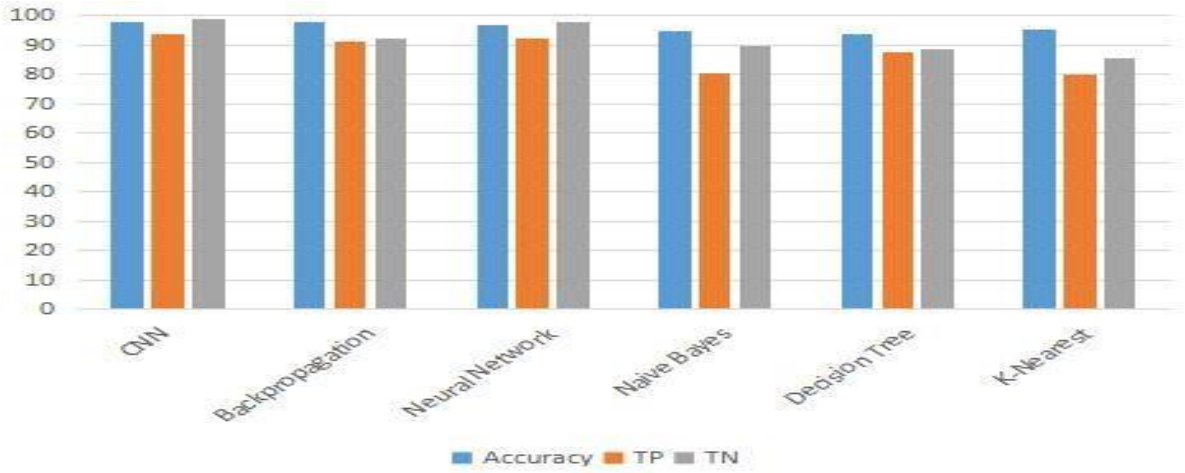


Figure 12. **Developed and previously implemented Algorithms**

4.0

CONCLUSION

Smishing has shown to be a very effective attack on mobile users and has the ability to seriously harm both people and businesses. Consequently, as demonstrated in the experiments, the Convolutional Neural Network smishing detection model developed and integrated into

a mobile application can track and detect smishing-related messages, preventing mobile users from becoming victims of smishing attackers. This study successfully developed a smishing detection model for mobile application. This model has demonstrated effectiveness in detecting smishing attacks by capturing both local patterns and long-term dependencies in text messages. The incorporation of CNN has notably improved the model's performance accuracy compared to traditional machine learning approaches.

5.0 RECOMMENDATIONS

However, future research efforts should focus on reducing the latency in detecting smishing messages to enable real-time prevention and response. Investigate edge computing solutions to process data locally on mobile devices. It is also recommended to develop automated response mechanisms that not only detect but also respond to smishing attempts by alerting users or blocking malicious messages in real-time. Lastly, Extend the smishing detection capabilities to support multiple mobile operating systems beyond Android, such as iOS.

REFERENCES

Aljofey, A., Jiang, Q.; Qu, Q.; Huang, M.; Niyigena, J. (2020). An Effective Phishing Detection Model Based on Character Level Convolutional Neural Network from URL.

Babalola, H. (2022). ScienceDirect Development of a Real Time Smishing Detection Mobile Development of a Real Time Smishing Detection Mobile Application using

Rule Based Techniques Application using Rule Based Techniques. Procedia

Computer Science, 199, 95–102. https://doi.org/10.1016/j.procs.2022.01.012

Fachkha, C. (2023). Characterizing Mobile Money Phishing Using Reinforcement Learning.

IEEE Access, 11(August), 103839–103862. https://doi.org/10.1109/ACCESS.2023.3317692

Gadde, S. (2021). SMS Spam Detection using Machine Learning and Deep Learning Techniques. 358–362.

International, A., Ghazi-tehrani, A. K., Pontell, H. N., and Ghazi-tehrani, A. K. (2021). Phishing Evolves : Analyzing the Enduring Cybercrime Phishing Evolves : Analyzing the Enduring Cybercrime ABSTRACT. Victims and Offenders, 16(3), 316–342.

Janulevi˘, J. (2020). applied sciences E-mail-Based Phishing Attack Taxonomy. 1–15.

Mishra, S., and Soni, D. (2020). Smishing Detector : A security model to detect smishing through SMS content analysis and URL behavior analysis. Future Generation

Computer Systems, 108, 803–815. https://doi.org/10.1016/j.future.2020.03.021

Mishra, S., and Soni, D. (2021). DSmishSMS-A System to Detect Smishing SMS. Neural Computing and Applications, 0123456789. https://doi.org/10.1007/s00521-02106305-y

Mishra, S., and Soni, D. (2022). Implementation of ‘ Smishing Detector ’: An Efficient Model for Smishing Detection Using Neural Network. SN Computer Science, 3(3), 1–

13. https://doi.org/10.1007/s42979-022-01078-0

Wahsheh, H. A. M., and Al-zahrani, M. S. (2022). Lightweight Cryptographic and Arti fi cial Intelligence Models for Anti-smishing.