DOI: http://dx.doi.org/10.26483/ijarcs.v17i3.7439

ISSN No. 0976-5697

Volume 17, No. 3, May-June 2026

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A MULTILINGUAL WEB-BASED SMS PHISHING DETECTION SYSTEM TAILORED TO THE NIGERIAN THREAT LANDSCAPE

Alfred Akpan Udosen, Oluwatomilola Mojolaoluwa Arogundade*, Ayomide Solomon Afolayan, Oluwaferanmi Victor Osinibi, Christiana Jumoke Daramola

Department of Computer Science,
Babcock University
PMB 4003, Ilishan-Remo Ogun State, Nigeria.

Abstract: With mobile communications becoming part of Nigerian daily life, SMS phishing attacks are taking a huge turn for the worse, targeting unsuspecting users with fraudulent messages that trick them into providing personal and financial information. This study proposes a user-centric SMS phishing detection system tailored to the Nigerian context to design and implement an intelligent and user-friendly solution capable of accurately detecting phishing SMS messages and to raise user awareness using multilingual messages and easy feedback channels. The four classification algorithms trained and tested were Support Vector Machine (SVM), Random Forest, Multinomial Naive Bayes and Logistic Regression, whose performance metrics were accuracy, precision, recall, F1-score and Area Under the ROC Curve (AUC-ROC). Cross-validation was employed to ensure reliability and generalisability of the model. The result obtained from the models showed that the Support Vector Machine model performed best with the highest overall accuracy and good generalisation error in the classification of high-dimensional text data; thus, it was selected as the final model to be deployed. To enhance access by multiple user groups, the system was further enhanced by the provision of a web-based interface, several Nigerian language supports, visual warnings, and audio prompts. In conclusion, the developed system correctly identifies phishing messages and provides an easy way to reduce fraud on mobile devices in Nigeria. Future research should focus on expanding the dataset with more native language samples, adding deep learning models to improve multilingual understanding and partnering with telecommunication firms to make real-time fraud prevention and extensive use.

Keywords: Detection System, Landscape, Multilingual, Nigeria, Phishing, Support Vector Machine, Threat

I. INTRODUCTION

A. Background to the Study

The Short Message Service (SMS) remains one of the most popular communication channels worldwide due to its cost-effectiveness, simplicity, and compatibility with all mobile devices. But as mobile communication use increased, so did the use of SMS for fraudulent purposes. Notably, the rise of mobile use around the world has led to an increase in instant messaging scams with considerable socioeconomic harm. Cybercriminals use SMS smishing to impersonate banks, telecommunications providers or government agencies to trick recipients into giving up private information or transferring money.

Even though any individual is vulnerable to online scams, recent data suggests that younger individuals are at greater risk as they are more inclined to interact with fraudulent content, such as clicking on dangerous links, because they often use digital platforms and have little experience detecting fraudulent behaviour. The current defences, predominantly relying on static keyword filtering, cannot cope with the language variability and new techniques of these scammers, given the rise of artificial intelligence. Artificial intelligence (AI), machine learning (ML) in particular, and natural language processing (NLP) offers a more flexible and intelligent way of detecting scam messages.

B. Statement of the Problem

Youth and young adults are increasingly the main target of sophisticated SMS-based scams (smishing), especially those with a banking focus, despite their widespread digital fluency. Nigerian youth are more vulnerable to cyber fraud risks due to economic pressures, with 33.3% unemployment among 18-35-year-olds [1] pushing desperate job seekers into fake recruitment scams [2]. The 217% rise in account breaches among young adults between 2021 and 2023 reported by CBN can be attributed to a lack of digital literacy, as many are unable to identify phishing attempts posing as bank alerts or job offers [2]. Current preventive measures, like generic awareness campaigns and simple built-in spam filters, are largely inadequate given their reactive nature and the inability to adapt to the rapidly changing tactics used by fraudsters [3]. Young people are prone to identity theft, financial exploitation, and extreme emotional distress because of their unique digital habits and irregular overconfidence in their ability to identify online threats. Therefore, there is an urgent need for a proactive, intelligent,and personalized web application that leverages the capabilities of AI to issue real-time alerts for smishing attempts related to finance to empower and protect young adults against online fraud.

C. Aim and Objectives

This study aims to design and develop an artificial intelligence-based web application to display alerts for short

message service-based scams to raise the financial literacy and digital security of the youth. The particular objectives are to:

1. design a scalable and modular system architecture for the scam prevention tool.
2. implement the designed system in (1).
3. evaluate the implemented system in (2).

II. LITERATURE REVIEW

A. History of Short Message Service Scams

Scams involving short message services, also known as "smishing" (a combination of "SMS" and "phishing"), have become a common type of online fraud. Fraudulent text messages are used in these scams to trick people into divulging private information, downloading malware, or clicking on harmful links [4] that makes them vulnerable to online attacks. Scammers have discovered new ways to take advantage of people who might not be as watchful on mobile platforms as they are with emails due to the increased reliance on mobile communication in both developed and developing nations.

Smishing attacks have become more context-specific and localised, particularly in Nigeria, where mobile phone and mobile banking adoption rates are rising quickly. Basically, these scammers often use urgent or emotionally charged language to manipulate recipients while posing as reputable organisations, such as banks and telecom providers [5]. To boost credibility, linguistic and cultural cues like community-based framing or religious appeals are frequently employed [6].

The continued presence of Short Message Service scams suggests that while different measures have been implemented, including the adoption of machine learning algorithms for detection and awareness campaigns for users, the scams have remained effective in their heinous acts. Studies show that mobile users are still highly susceptible because of their low digital literacy, weak regulatory compliance, and the simplicity of using the technology known as Short Message Service (SMS) [7]. This literature review discussed the nature of the smishing attacks, who they target, the scammers' psychological and cultural approach, the impact of smishing on the banking industry, and the effectiveness of technical and non-technical interventions.

The banking sector is a major victim of SMS-based scams, as it is so mobile-focused that it is essential for communicating with customers and conducting transactions. Consequently, financial institutions are increasingly expanding their financial services in developing countries like Nigeria [8], and the end-user devices, including smartphones, that they use to access those services are becoming increasingly vulnerable to cybercriminal activities.

Smishing attacks typically bypass typical network-level security protocols because they target the end user instead of the network, and due to human error and a lack of digital awareness, many attacks with relatively low sophistication, such as simple text messages with urgent calls to action, can still be very successful. Without any form of suspicion, a lot of people often click on links without verifying their source, they do not use anti-malware software, and do not regularly update their devices. These behaviours are typical vulnerabilities in otherwise secure banking infrastructures, as endpoint devices are often the weakest link.

Once breached, a device can be a conduit for accessing valuable banking apps, SMS two-factor authentication (2FA), and credentials stored on the device. In addition, if the end-user is somehow responsible for the attack, smishing attacks targeting banking applications could result in financial loss and will cause harm to the organisation's reputation. To tackle this, banks are putting more resources into endpoint solutions such as app-based 2FA, biometric verification, awareness and education initiatives, and AI-powered fraud monitoring [9].

B. Machine Learning in SMS Scam Detection

With an ever-growing arsenal of fraudsters' techniques to target mobile users, machine learning has become an important tool for SMS scam detection and prevention. In contrast to the rule-based system, machine learning algorithms can automatically recognise patterns and anomalies in text messages, thus improving and flexibly filtering spam messages.Notably, it is often supervised learning methods that are employed in training a model from a labelled dataset with examples of acceptable messages and spam messages. Furthermore, deep learning models and hybrid architecture have been proven to be able to learn the sequential and local patterns so as to obtain high level of accuracy performance. They tend to be compute heavy with a need for large labelled datasets; however, making them hard to scale in low-resource areas. Also, the lack of regional support for current commercial solutions, makes such systems often not accessible to older, low-literate people.

III. SYSTEM ANALYSIS AND DESIGN

A. Research Design and System Architecture

A Design Science Research (DSR) methodology was used to develop a usable tool to address a real-world SMS scam problem, particularly for multilingual and underserved users. The process was the cyclical process of problem identification, artefact design, demonstration, evaluation, and communication. The system was developed to be a proactive web application, breaking away from mobile constraints to provide greater access. They consist of the following parts:

1. Message Input Module: This part receives all the messages from the user and extracts the number and the content of the message for pre-processing.
2. Machine Learning Detection Engine: This uses support vector machine model that was trained to identify specific patterns according to local keyword structures and classify texts.
3. Alert System: This identifies the possible scam messages and informs the user through visual overlay and sounds in the local language of the user's choice.
4. Preferences & Language Manager: This part stores user preferences for languages used in the interface (English, Pidgin, Yoruba, Hausa and Igbo) and voice alert options.

B. Data Preprocessing and Feature Extraction

The Nigerian SMS spam data set that was collected locally as well as the SMS Spam Collection from Kaggle [10]. This dataset includes a mixture of phishing and non-phishing

SMS messages, and the unstructured data is subjected to strict and rigorous data pre-processing in the following manner:

1. Punctuation Removal: It identifies and removes symbols and special characters that do not convey meaning.
2. Numerical Removal: It removes digits that may mislead text feature extraction.
3. Lowercase: It makes every text lowercase, for consistency.
4. Stemming: This shortens words to their stems.
5. Stop-Word Removal: Removes words which are frequent but do not have any meaning.

After pre-processing, the text is converted to numerical parameters by term frequency–inverse document frequency (TF-IDF) vectorisation.

IV. IMPLEMENTATION AND MODEL EVALUATION

A. Model Selection and Training

Four supervised machine learning algorithms were trained: Support Vector Machine (SVM), Random Forest (RF), Multinomial Naive Bayes (MNB), and Logistic Regression (LR). This dataset containing 4,981 labelled SMS messages (2,805 legitimate and 2,176 spam) was provided and divided into an 80% training set and a 20% testing set. To reduce overfitting and increase reliability, a 5-fold cross-validation was carried out in the training phase.

B. Comparative Model Performance

The Support Vector Machine (LinearSVC) model was chosen for the web application because it made the best balance between false-positive and false-negative errors, which is important in a public-facing fraud detection system, and it performed best in experimental comparisons. It demonstrated the best compromise between false-positive and false-negative errors, which is important for a fraud detection system that is to be used by the public. The table below shows the performances of the different models used in the study.

Table 1

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC
SVM (LinearSVC)	92.48%	90.00%	91.51%	91.41%	0.9713
Random Forest	92.28%	91.00%	90.60%	91.12%	0.9674
Logistic Regression	90.97%	90.76%	94.04%	90.11%	0.9653
Naive Bayes (MNB)	92.58%	91.00%	94.04%	91.72%	0.9720

*Note: Naive Bayes was ultimately disqualified due to feature incompatibility during live inference, despite producing competitive benchmark metrics.

C. Web Application Interface

The web app, FraudLock, uses a trained SVM model with a Python (Django) backend and a React.js frontend. The UI is designed to be accessible to the users through:

1. Fraud Detection Interface: This enables pasting an SMS into the text box and then pressing the “Analyse Message” button. The system returns a colour-coded result (red if spam and green if legitimate), a confidence percentage and a fraud category (e.g., "Bank / Identity").
2. Multilingual Support: The whole interface can be translated into English, Nigerian Pidgin, Yoruba, Hausa or Igbo.
3. Number Intelligence & Reporting: Its users are able to search numbers in Nigeria for their fraud history and report suspicious numbers, and any number with more than twenty reports will be automatically marked for telecom blocking.
4. Admin Dashboard: System administrators are given an advanced view of total scans, detection rates, and a feedback loop to retrain the model based on reported false positives.

D. System Overview

The following section provides a view of the structure comprising all the components and their relationships, along with the flow of data that will be part of the proposed system. This section is going to serve as the technical design for developing the web application scam prevention system targeting people of Nigeria for fraud related to banking through AI-enhanced keyword classification. The main components include:

1. Message input module: The job of this component is to handle all the messages that arrive via typing or pasting via the user’s input. This component extracts the number and the message itself once the message is received. The purpose of the Message Input Module is to preprocess and filter the data that is given to the machine learning detection engine.

2. Machine learning detection engine: This major component is designed to scan the incoming SMS messages for potential scam messages. This classification is done with

the aid of a keyword recognition system, which is trained with known scam patterns, like “your BVN has been blocked”, “your account is locked; click here to unlock”, and “urgent OTP”. By utilising natural language processing and supervised learning, our approach will develop a technique to classify messages as either spam or legitimate messages, utilising non-technical patterns and statistical information in the message content. A publicly available Short Message Service will be utilised in learning and testing to determine accuracy and efficiency, utilising Random Forest Classifiers, among others. The engine then searches the message for these patterns to determine the likelihood of a message being a potential scam, and if the message is considered a scam, the engine then goes ahead to notify the user. Also, the engine will be totally offline, meaning speed and privacy will be maintained and protected.

3. Alert System: The alert component alerts the user when a possible scam message is identified. It can use alerts, system notifications, or overlay alerts, for instance, “Dismiss” and “Report”. The alert can also give voice alerts in a locally preferred language, for instance, Yoruba & Hausa, making the system more ideal for less literature-prepared users.

4. User Interface (UI): This component will handle all interactions with the user, as it is set to offer an interactive interface for users so as to view detected messages, manually report suspicious messages, and set language and alert preferences, as well as view the history of scam messages. The interface for this system is set to be developed using HyperText Markup Language 5, Tailwind CSS, and JavaScript/TypeScript, which are going to create all interactions for the user interface. It is set to offer the scam history view and current alert displays and be the interface for the preferences manager.

5. The Preferences & Language Manager module will be responsible for storing the user preferences related to interface languages, voice alert options, and the sensitivity level for scamming. It will allow the users to customise the system and make it user-friendly to the users of a different culture in Nigeria.

6. Security and Privacy Considerations: Privacy is the highest priority of the design; all detection is done through optics, with no cameras visible to the user. Storage and analysis of message data are not uploaded to a cloud server. Secure permissions are enforced, and everyone should opt in to sharing their data.

Figure 1 shows the landing page of the application. It offers users an overview of the system and enables them to navigate to different features such as message analysis and number intelligence.

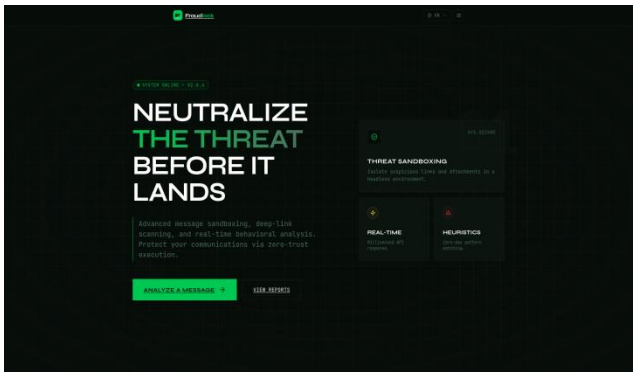

Figure 1: The home page of Fraudlock

The system as shown in figure 2 is multi-lingual. It displays the interface in the language of Nigerian Pidgin and has a drop-down menu to choose other languages to enhance accessibility.

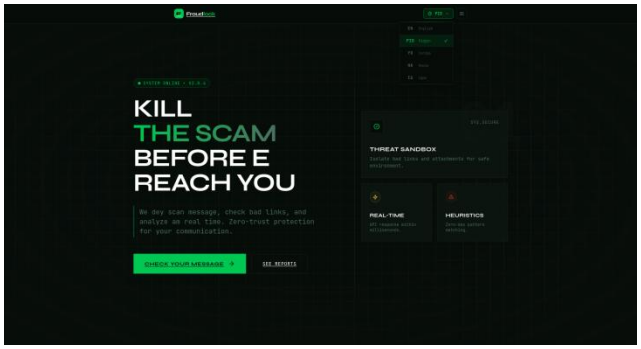

Figure 2: Dropdown menu for the multilingual user interface and the Pidgin text.

Figure 3 shows the results of an analyzed SMS message. It indicates if the message is phishing or not. A legitimate and a confidence score, and then some indicators. The system comprises a machine learning

model to predict the probability of spam messages from data provided by the user. The model takes input as follows: To create an output in percentage format (messages).

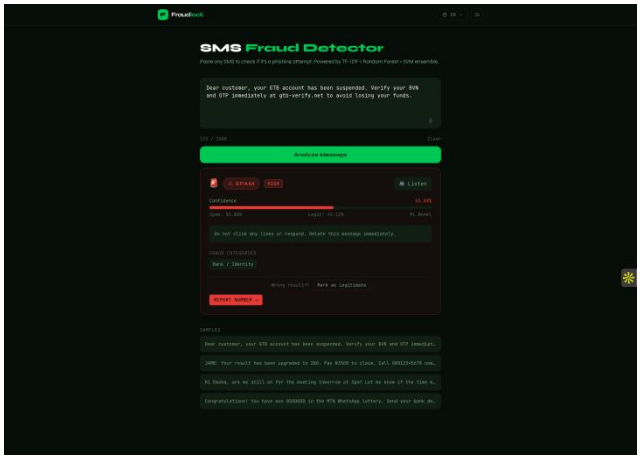

Figure 3: The Result page displaying the result of an analysed message.

V. CONCLUSION AND RECOMMENDATIONS

CONCLUSION

The creation of this online application to stop scams using the help of artificial intelligence has proven that machines can build applications that are better at preventing scams than humans.

The Support Vector Machine algorithm, in conjunction with TF-IDF vectorisation were used iin this case and offers a good way to detect fraudulent SMS activity. By adopting a web-based architecture, the system ensures broad accessibility. Also, the addition of multilingual support, visual cues; this reflects inclusivity.

Effective community reporting changes the reporting paradigm from a reactive one to a real-time proactive detection one, which is suitable to the Nigerian demographic.

RECOMMENDATIONS

The following are recommended to further improve the SMS scam prevention system:

1. On-Device Processing: Develop lightweight, on-device machine learning models that can function even without the internet connection, thus lowering the latency for end-users.
2. Crowdsourced Databases: Add to the platform's functionality to support crowdsourced scam reports. In real-time, the active model can be retrained on new threats and patterns.
3. Industry Integration: Nigerian banks and telecommunication providers should consider integrating the API of this system into their official systems to offer a single source of endpoint security for their customers, thereby assisting in the growth of this industry.

VI. REFERENCES

[1] National Bureau of Statistics (NBS), “Nigeria Labour Force Survey Q4 2023,” Abuja, Nigeria, 2023.

[2] iTelemedia, “Fake Job Recruitment Scams Targeting Nigerian Youth", 2025. [Online]. Available: https://itelemedia.com/. [Accessed: May 19, 2026].

[3] Muhammad, S., Muhammad, I., & Mohamed Ali, K. (2024). Investigating evasive techniques in SMS spam filtering: A comparative analysis of machine learning models. *IEEE Access, 12*, 24306–24324.

[4] 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. 199, pp. 95–102, 2022.

[5] E. Carter, “Confirm Not Command: Examining Fraudsters’ Use of Language to Compel Victim Compliance in Their Own Exploitation,” The British Journal of Criminology, vol. 63, no. 6, pp. 1405–1422, 2023, doi: 10.1093/bjc/azac098.

[6] T. M. Ajayi, “Discursive-manipulative strategies in scam emails and SMS: The Nigerian perspective,” Lodz Papers in Pragmatics, vol. 18, no. 1, pp. 175–195, 2022, doi: 10.1515/lpp-2022-0008.

[7] T. Mahmud, M. A. H. Prince, M. H. Ali, M. S. Hossain, and K. Andersson, “Enhancing Cybersecurity: Hybrid Deep Learning Approaches to Smishing Attack Detection,” Systems, vol. 12, no. 11, p. 490, 2024, doi: 10.3390/systems12110490.

[8] N. V. Ezechukwu, “Regulating Innovation for Financial Inclusion: Lessons from Nigeria,” Journal of African Law, vol. 65, no. 3, pp. 365–387, 2021, doi: 10.1017/S0021855321000279.

[9] T. O. Ogunleye and A. Y. Alimi, “Artificial Intelligence Techniques for Fraud Detection and Prevention in Digital Financial Systems,” International Journal of Advanced Computer Science and Applications, vol. 13, no. 9, pp. 522–530, 2022.

[10]A.Alli, “SMS Spam Dataset,” GitHub repository. [Online].Available: https://github.com/AbayomiAlli/SMS-Spam-Dataset.

