ASEC
2025
Conference

The 6th International Electronic Conference on Applied Sciences

09–11 December 2025 | Online

MDPI

AN ENHANCED SMS PHISHING DETECTION MODEL USING DEEP LEARNING.

Abdullahi Ishaq[1*], Zaharadden Salele Iro[2], Aminu Musa[1], Abida Auba[1], , Bilal Ibrahim Maijamaa[1], Abubakar M Miyim[2],

1 Department of Computer Science, Federal University Dutse, Dutse 720211, Nigeria

2 Department of Information Technology, Federal University Dutse, Dutse 720211, Nigeria

INTRODUCTION & AIM

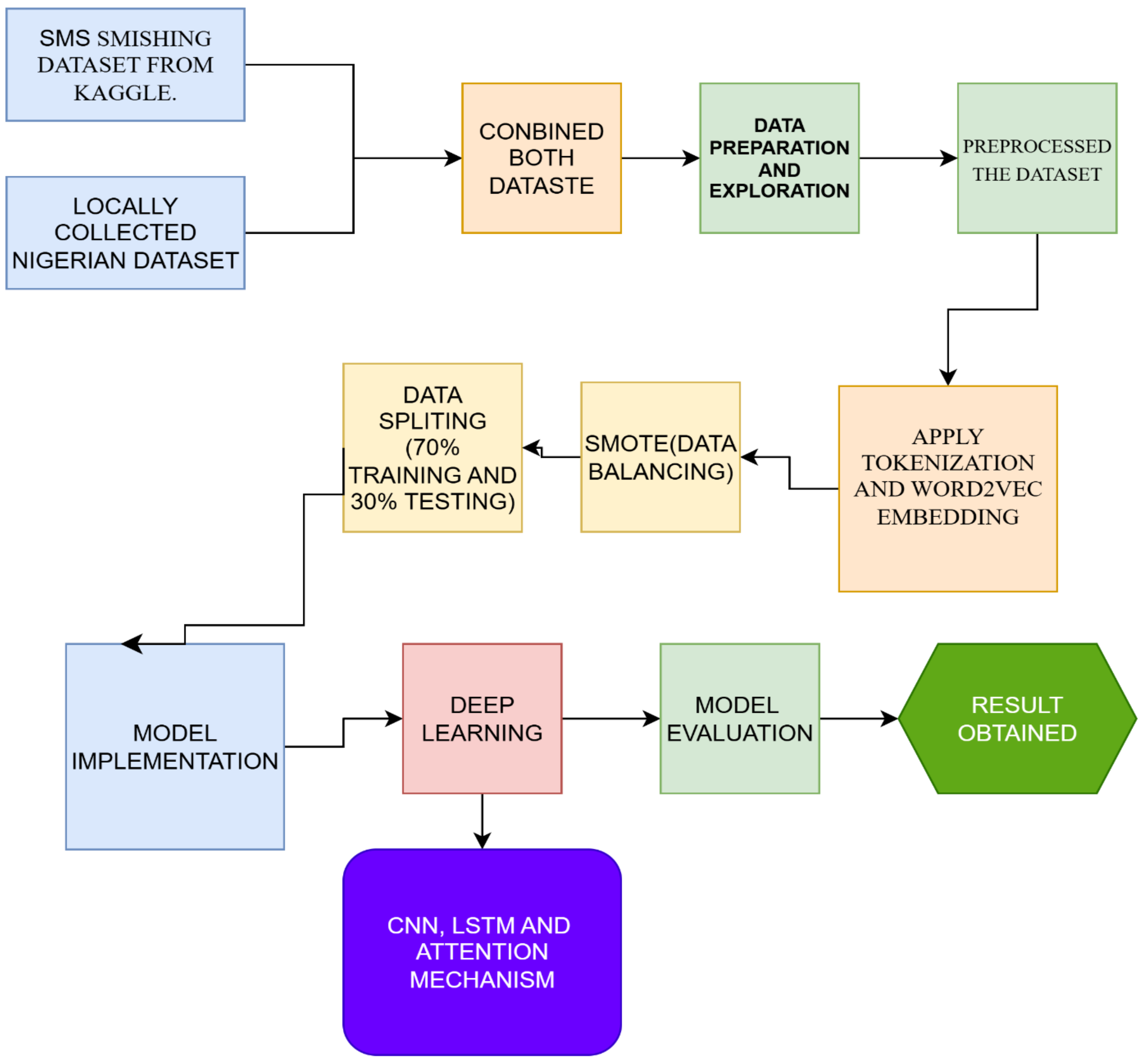
Short Message Service (SMS) is still a vital communication tool in our daily life activities, even with the quick development of Internet protocol-based messaging services. An increasingly sophisticated cyber threat known as SMS phishing (smishing) has emerged in tandem with the rise in mobile device use

phishing is an attack targeted to mobile devices in which the attacker sends text messages containing malicious links, phone numbers or E-Mail IDs to the victim and the attacker aims to steal sensitive user data like bank account details, passwords, user credentials, credit card details,

This research aims to develop an enhanced sms phishing detection to enhance protection against SMS phishing attacks within the Nigerian context. the goal is to develop an effective SMS phishing detection system to accurately detect and categorize SMS phishing messages.

METHOD

The study developed a system for detecting fraudulent SMS messages using a structured methodology. Two datasets were combined: one from the Kaggle Smishing Collection and another containing real Nigerian smishing samples to ensure local relevance. Data preparation involved removing duplicates, handling missing entries, confirming correct labels, cleaning text, and applying lemmatization. Labels were then converted into numeric form. Messages were transformed into word vectors using tokenization and Word2Vec, while SMOTE was applied to correct class imbalance. The processed dataset was divided into training (70%), testing (15%), and validation (15%) sets. Three classification models CNN, LSTM, and Attention-based architecture were implemented and compared. Their performance was measured using precision, recall, accuracy, and F1-score.

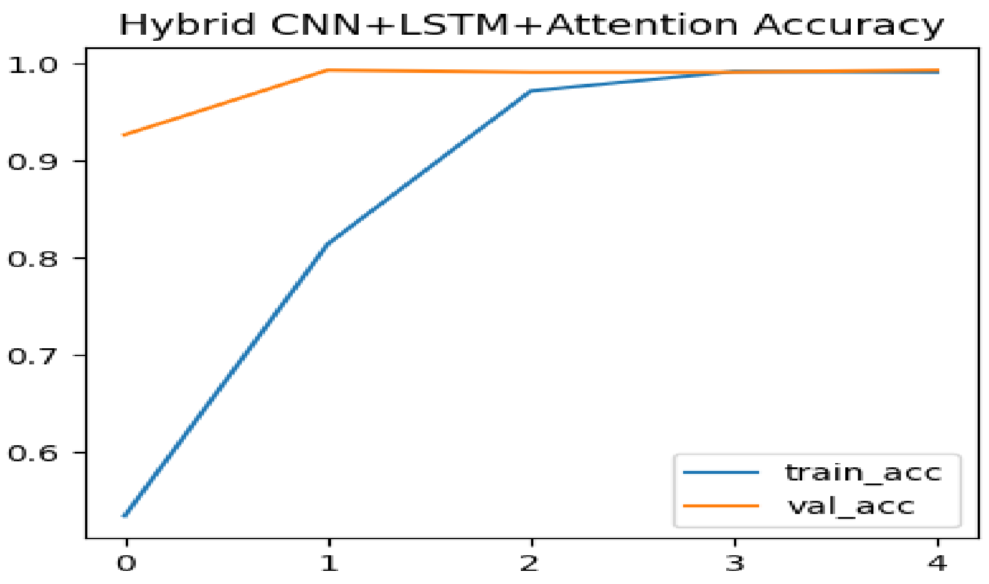

SMS SMISHING DATASET FROM KAGGLE.
LOCALLY COLLECTED NIGERIAN DATASET
CONBINED BOTH DATASTE
DATA PREPARATION AND EXPLORATION
PREPROCESSED THE DATASET
APPLY TOKENIZATION AND WORD2VEC EMBEDDING
SMOTE(DATA BALANCING)
DATA SPLITING (70% TRAINING AND 30% TESTING)
MODEL IMPLEMENTATION
DEEP LEARNING
MODEL EVALUATION
RESULT OBTAINED
CNN, LSTM AND ATTENTION MECHANISM

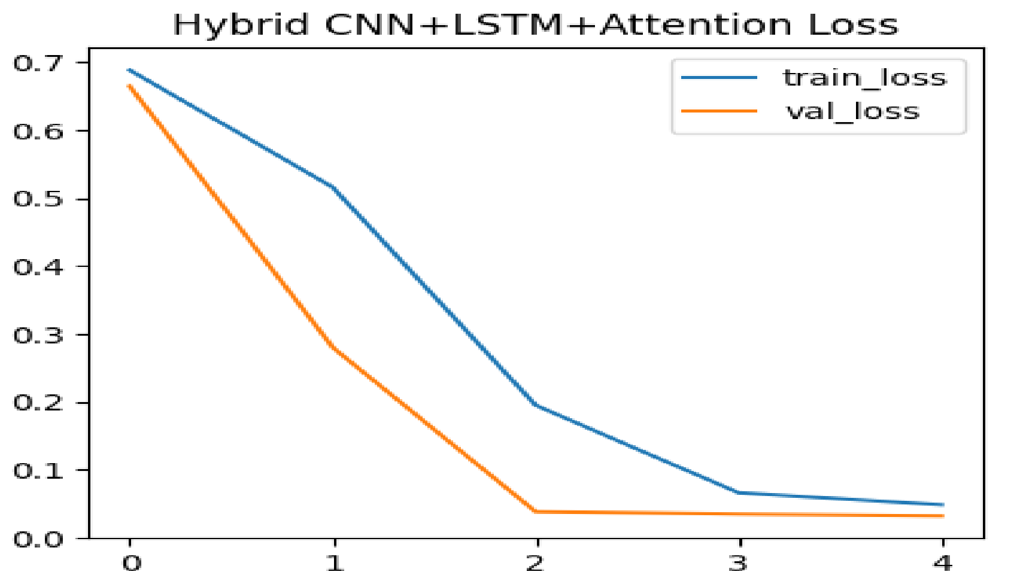
PROPOSE FRAME WORK

RESULTS & DISCUSSION

The hybrid detection system performed strongly overall, yet further review exposed notable weaknesses. Most errors were false negatives, especially when fraudulent messages closely resembled genuine SMS by using friendly language, shortened links, or well-structured sentences. False positives appeared when real messages carried urgency or contained links, causing the system to mistake them for threats. These issues suggest the model still lacks full contextual understanding. Furthermore, although CNN, LSTM and Attention-based models achieved the highest accuracy and precision, their effectiveness shifted with changes in class balance and message complexity.

The hybrid combination of CNN, LSTM and Attention outperformed single CNN models for SMS scam detection, especially with short text messages where feature-based learning is more effective. Limited dataset size reduced overall capability, showing the need for larger data and augmentation. The study provides useful findings but requires further refinement for real-world application. Performance could improve with mobile integration, user feedback, real-time monitoring, and stronger defense techniques to counter evolving phishing attacks.





Model	Accuracy	Precision	Recall	F1 score
CCN	98.62%	100%	98.08%	99.03%
LSTM	71.95%	71.95%	100%	83.69%
ATTENTION	98.85%	100%	98.4%	99.19%
HYBRID OF CNN+LSTM+ATTENTION	99.31%	100%	99.08%	99.52%

RESULT COMPARATIVE ANALYSIS

CONCLUSION

The rise of mobile phones and SMS use has led to increased smishing attacks that threaten privacy and finances. In Nigeria and elsewhere, these attacks have grown more sophisticated, making them harder to detect. This study addressed the problem by creating and testing a system designed to automatically identify and classify fraudulent SMS messages.

FUTURE WORK / REFERENCES

Future work should deploy the smishing detection system in real environments with telecom and banking networks to test its scalability. Advanced text-based models like BERT and RoBERTa may improve performance but need optimization for low-resource, real-time use. Regular retraining is required to handle evolving phishing styles, along with stronger defense against evasion attacks. Privacy protection, secure data handling, and lightweight deployment design will be crucial for reliable long-term operation