



SCHOOL OF COMPUTING, TECHNOLOGY AND APPLIED SCIENCES

**A SMISHING ATTACK DETECTION MODEL FOR MOBILE MONEY BASED
ON NATURAL LANGUAGE PROCESSING AND MACHINE LEARNING**

KATONGO ONGANI PHIRI

A Final Year Research Project submitted in partial fulfilment of the requirements for
the degree of

Master of Science in Computer Science

ZCAS UNIVERSITY

2023

DECLARATION

Name: KATONGO ONGANI PHIRI

Student Number: ZU18180

I hereby declare that this final year research project is the result of my own work, except for quotations and summaries which have been duly acknowledged.

Plagiarism check:9%

Signature: k.phiri

Date: 31/12/2023

Supervisor Name: Dr Zimba

Supervisor Signature:

Date:

A SMISHING ATTACK DETECTION MODEL FOR MOBILE MONEY BASED ON NATURAL LANGUAGE PROCESSING AND MACHINE LEARNING

ABSTRACT

As mobile money services proliferate, the threat of smishing attacks targeting users has escalated. This paper presents a Smishing Detection Leveraging Natural Language Processing (NLP) and Machine Learning (ML) techniques. It aims to detect smishing threats in real-time with the integration of an Android App. The model harnesses NLP algorithms to analyse text-based messages, scrutinizing linguistic patterns and contextual cues indicative of smishing attempts. Through ML algorithms, the model learns to distinguish between legitimate (Non-Smishing) and fraudulent messages (Smishing), adapting dynamically to evolving smishing tactics. The model's efficacy is evaluated through comprehensive testing, demonstrating promising accuracy, precision, and recall rates. The Model stands as a proactive defense mechanism against smishing in mobile money environments, contributing to enhanced user security and trust in financial transactions.

Keywords: Smishing, Non-Smishing, Detection, Model, NLP, ML

ACKNOWLEDGEMENT

I would like to take this opportunity to express my gratitude and appreciation to my supervisor, Dr Zimba for the guidance, patience and invaluable advice throughout this project.

THANK YOU.

DEDICATION

I would like to take this opportunity to express my gratitude and appreciation to my family and friends for the supported rendered during the research.

Table of Contents

CHAPTER 1 : INTRODUCTION	11
1.1 Background to the study	11
1. 2 Problem Statement.....	13
1.3 Aim	13
1.4 Objectives of the Study.....	14
1.5 Research Questions:.....	14
1.6 Scope and Limitation	15
1.7 Significance of the Study	16
1.8 Preliminary sections of the project report.....	17
CHAPTER 2: LITERATURE REVIEW	18
2.1 General Background	18
2.2 Broad literature review of the topic	19
2.3 Critical review of related works.....	20
2.4 Conceptual framework/Theoretical framework.....	22
2.5 Proposed model/system	23
2.6 Comparison with related works	24
CHAPTER 3: METHODOLOGY	26
3.1 Research Design.....	26
3.2. Adopted Method and Justification.....	26
3.3 Association Of Methods To Project.....	27
4.4 Research Data And Datasets:.....	27
CHAPTER 4: DATA, EXPERIMENTS AND IMPLEMENTATION	36
4.1 Appropriate Modeling In Relation To Project.....	36
4.2 Techniques, Algorithms, Mechanisms.....	38
4.3 Implementation:	39
CHAPTER 5 RESULTS AND DISCUSSIONS.....	51
5.1 Results Presentation	51
5.2 Analysis of Results.....	54
5.3 Comparison of Results to Related Work.....	56
5.4 Implication of Results:.....	56
CHAPTER 6: SUMMARY AND CONCLUSION	59
6.1. The Research Had The Following Findings	59
6.2. Contribution to the Body of Knowledge: Leveraging Nlp and Ml.....	60
6.3 Limitations of the Research Project:.....	61

6.4 Future Works: Advancements and Development	62
6.5 Conclusion: The Ongoing Battle against Smishing in Mobile Transactions.....	64
REFERENCES	66

LIST OF TABLES

1. TABLE 2.1 COMPARISON WITH RELATED WORKS – P25
2. TABLE 3.1 ENGLISH SMISHING DATASET - P35
3. TABLE 3.2 BEMBA SMISHING DATASET – P36
4. TABLE 5.1 MODEL METRIC PERFORMANCE: - P54
5. TABLE 5.2 COMPARISON OF RESULTS TO RELATED WORK – P57

LIST OF FIGURES

1. FIGURE 1.0: SMS TRAFFIC VISUALIZATION FROM 2011 TO 2022 (ZICTA, 2023) – P12
2. FIGURE 2.1 POPULATION VS ACTIVE SUBSCRIBERS (ZICTA, 2023) – P19
3. FIG 3.1 MOBILE MONEY NETWORK USAGE – P29
4. FIG 3.2 MESSAGE LANGUAGE – P30
5. FIG 3.3 SMISHING AWARENESS – P31
6. FIG 3.4 NUMBER OF RECEIVED SUSPICIOUS MESSAGE – P32
7. FIG 4.1 SMISHING ARCHITECTURE - P40
8. FIG 4.2 SMISHING DETECTION FLOWCHART –P43
9. FIG 4.3 ANDROID APP FLOWCHART –P46
10. FIG 4.4 ANDROID APP UI – P49
11. FIG 4.5 TELNET CMD SMS SENDING SIMULATION – P49
12. FIG 4.6 MESSAGE RECEIVED AND RESPONSE OF RESULT – P50
13. FIG 4.7 FLASK APP RUNNING UPON RECEIVED POST REQUEST – P51
14. FIG 5.1 BEMBA SMISHING WORD CLOUD - P52
15. FIG 5.2 ENGLISH SMISHING WORD CLOUD – P53
16. FIG 5.3 RANDOM FOREST ROC CURVE – P54
17. FIG 5.4 NAÏVE BAYES ROC CURVE FIG – P54
18. FIG 5.5 LOGISTIC REGRESSION ROC CURVE – P55

LIST OF ABBREVIATIONS

1. ML
2. NLP
3. MM

CHAPTER 1 : INTRODUCTION

1.1 Background to the study

In today's world, smartphones have gained immense popularity because of their small and easily portable design, along with their extended battery life. In Zambia, the liberalisation of the telecoms sector and the subsequent introduction of multiple mobile network providers saw the widespread adoption of mobile phones (Zimba et al. 2020). This surge in smartphone adoption has resulted in a higher prevalence of SMS and instant messaging as the primary means of communication (Goel & Jain, 2018). Among these, SMS stands out as the most commonly utilized and widespread text-based communication service. According to Zicta statistics (Zicta 2023), the number of incoming SMS messages increased by approximately 974.3% from 2011 to 2022, with a minimum of 101.21 million in 2013 and a maximum of 1,088.01 million in 2022. Outgoing SMS messages also experienced significant growth, with a staggering increase of approximately 3334.4% from 2011 to 2022. The data ranged from a minimum of 30.52 million in 2013 to a maximum of 1,047.85 million in 2022. This surge in SMS traffic highlights the enduring importance of text-based communication as it is a simple and inexpensive feature, and available on all mobile phones (Pour, Ehsan Rahmani, Aliyari, Shahla, Farsi, Zahra, & Ghelich, 2020). The diagram in Figure 1.0 shows a visualization of the surge in SMS traffic highlighting the enduring importance of text-based communication.

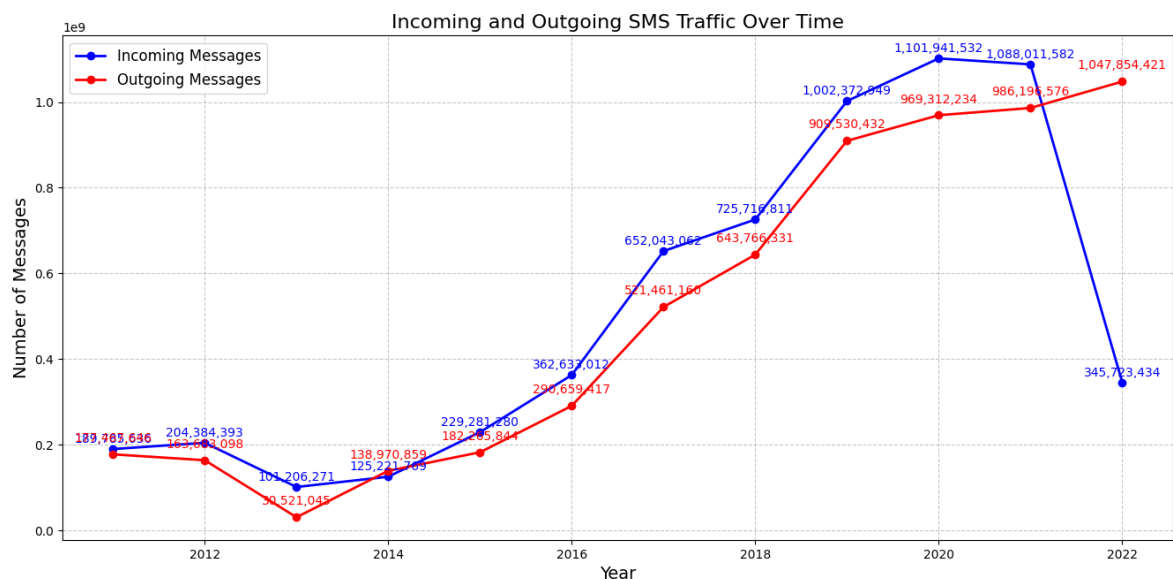


Figure 1.0: SMS Traffic Visualization from 2011 to 2022 (Zicta, 2023)

Mobile money technology is a method for transferring payments via mobile phones. This technology represents a financial innovation that leverages Short Message Service (SMS) technology to compensate service providers using a commission-based system (Upadhyay & Jahanyan, 2016). With Mobile Money, a wide array of financial and banking operations can be carried out, encompassing activities such as buying airtime, paying utility bills and school fees, managing savings, and conducting mobile banking. According to Bank of Zambia (Bank of Zambia, 2023), Mobile money has experienced substantial growth, with the volume increasing significantly each year. The percentage change from 2012 to 2022 shows a tremendous 89.7% increase in Mobile Money transactions as compared to Electronic funds transfer which has had a percentage change from 2012 to 2022 of 9.7% indicating that Mobile Money has seen a wider adoption and has experienced much more substantial growth compared to Electronic Funds Transfer (EFT) over the years.

Mobile money in Zambia has produced a variety of socio-economic advantages. For instance, the growing adoption of mobile money services has led to enhanced financial inclusion, as reported by the Bank of Zambia in 2020. It has also created employment opportunities, particularly for the youth working as booth operators, according to (Kabala & Seshamani, 2016). Furthermore, mobile money has promoted a culture of savings, (Cooper, et al., 2019) and has served as a catalyst for entrepreneurial activities among small and medium-sized enterprises (SMEs).

Smishing, short for Short Message Service Phishing, is a form of phishing attack in which a malicious actor sends a text message, posing as a reputable entity, with the intent of acquiring sensitive information from the recipient for financial exploitation (Goel & Jain, 2017). Cyberattacks come in different forms not limited to password attacks, Denial of Service (DoS), Man-In-The-Middle (MITM), social engineering, etc. Social engineering stands out in the mobile phone landscape because it requires little technical knowledge or tools and is feasible both on feature and smartphones (Salahdine & Kaabouch, 2019). Social engineers take advantage of human behavioral vulnerabilities to benefit themselves. These individuals often use psychological tactics to manipulate users into complying with requests they would typically resist (Aleroud, Abu-Shanab, Al-Aiad, & Alshboul, 2020). Attackers favor SMS phishing because it is a trusted source during the exchange of confidential information by mobile subscribers (Delany, Buckley, & Greene, 2012; Sethi, Bhandari, & Kohli, 2017).

This study proposes a natural language processing and machine-learning based detection model to classify Bemba and English Smishing text messages targeting mobile money users. The contributions of this study, are organized and carried out under a real-world English and Bemba Smishing dataset collected from mobile money users in Zambia.

1. 2 Problem Statement

The increasing adoption of mobile money services has led to a surge in smishing attacks, where cybercriminals use deceptive SMS messages to target users, potentially causing financial loss, identity theft, and privacy breaches. Existing smishing detection methods primarily focus on email phishing and web-based attacks, neglecting the unique behavioral characteristics of smishing in SMS messages within the context of mobile money services. Over the past few years, there has been a noticeable trend where the total number of spam messages has surpassed that of spam emails (Sethi, Bhandari, & Kohli, 2017). This point is reinforced by an article featured in Forbes magazine, highlighting that responding to a text message takes around 90 seconds for a mobile phone user, whereas responding to an email typically requires 90 minutes (Weiss, 2021). Consequently, there is a critical need for the development of an effective and tailored smishing detection model that leverages natural language processing (NLP) and machine learning (ML) to accurately identify smishing attacks in mobile money systems. This research addresses the problem of the absence of a comprehensive and efficient solution for detecting smishing attacks in mobile money services in Zambia, which is essential for safeguarding the financial interests and personal information of users in this rapidly growing digital financial ecosystem.

1.3 Aim

The aim of this research is to develop a Smishing attack detection model for mobile money and enhance the security of mobile money users based on natural language processing and machine learning.

1.4 Objectives of the Study

1.4.1: To conduct a baseline study on Smishing Attacks

- Analyze historical data to identify patterns and trends in smishing attacks.
- Survey mobile money users to understand their experiences and perceptions of smishing threats.

1.4.2: To Review existing Smishing Models

- Identify and critically assess the methodologies and techniques used in previous smishing detection models.
- Evaluate the performance metrics and limitations of existing models to inform the development of an improved model.

1.4.3: To collect datasets, Bemba and English Corpus for the study

- Gather a comprehensive dataset of English smishing messages, ensuring diversity in content and sources.
- Curate a dataset of Bemba smishing messages, considering linguistic nuances and regional variations in the language.

1.4.4: To Develop and Evaluate the Model

- Implement natural language processing and machine learning algorithms capable of feature extraction and detection from collected datasets.
- Assess the model's accuracy, precision, recall, F1-score and using Matthews correlation coefficient to determine its effectiveness in detecting smishing attacks in both English and Bemba messages.

1.5 Research Questions:

Objective 1.5.1: To conduct a baseline study on Smishing Attacks

Q1: What are the historical patterns and trends in Smishing attacks based on the analysis of historical data?

- What are the experiences and perceptions of mobile money users regarding Smishing threats, as revealed through surveys?
- How do mobile money users' experiences and perceptions vary based on demographic factors such as age, gender, and usage frequency?

Objective 1.5.2: To Review existing Smishing Models

Q1: What are the methodologies and techniques used in previous Smishing detection models, and how do they compare?

- What are the performance metrics of existing Smishing detection models, and what are their limitations?
- How can the insights from existing models inform the development of an improved Smishing detection model?

Objective 1.5.3: To collect datasets, Bemba and English Corpus for the study

Q1: How can a comprehensive dataset of English Smishing messages be gathered to ensure diversity in content and sources?

- What linguistic nuances and regional variations should be considered when curating a dataset of Bemba Smishing messages?
- How can the quality and authenticity of the collected Smishing message datasets be ensured?

Objective 1.5.4: To Develop and Evaluate the Model

Q1: What natural language processing and machine learning algorithms will be implemented for feature extraction from the collected English and Bemba Smishing message datasets?

- How effective is the developed model in detecting Smishing attacks in English messages, and what are the accuracy, precision, recall, and F1-score results?
- How effective is the developed model in detecting Smishing attacks in Bemba messages, and what are the accuracy, precision, recall, and F1-score results?
- What are the potential challenges and limitations in developing and evaluating the model, and how can they be addressed?

1.6 Scope and Limitation

The coverage of this study is specifically limited to the detection of smishing attacks in two languages, English and Bemba, as they pertain to mobile money services in Zambia. Smishing attacks in other languages are beyond the scope of this research.

The choice of mobile money networks for this study, MTN Mobile Money and Airtel Money, was based on several factors. These two networks were selected due to their prominent

presence and usage in the geographic region under study. Additionally, both networks have a substantial user base and are recognized for their impact on the mobile financial services industry.

Model Development is applicable to mobile phone in that only text is needed which is available on any platform. One of the key advantages of this approach is that it solely relies on the analysis of text content within SMS messages. Text-based data analysis is a fundamental and widely supported feature across various mobile phone platforms and operating systems. Since text message capabilities are inherent to virtually all mobile phones, the proposed model can be readily applied to a wide range of devices, regardless of their make, model, or operating system. Furthermore, it aligns with the practicality of the research, ensuring that the smishing detection model can be implemented by a broad audience of mobile money users who may use different types of mobile devices. By not relying on specialized hardware or software requirements, the model's usability is maximized, making it an accessible and cost-effective solution for enhancing the security of mobile money transactions and communications on a diverse array of mobile devices.

The study is focused on developing a detection model in contrast to a prevention framework meaning the model is designed to detect and identify, as opposed to preventing the attacks issues from occurring.

1.7 Significance of the Study

In an era characterized by the ubiquity of mobile devices and the rapid evolution of digital financial services, the security of transactions conducted through mobile money platforms has emerged as a critical concern. SMiShing is a variant of phishing that employs text messages sent via mobile phones and smartphones as its primary mode of operation. It is a blend of 'SMS' (Short Message Service) and 'phishing,' where the perpetrator employs text messaging as the medium of choice, as opposed to email (Mishra & Soni, 2019).

(Elnaiem, 2019) delves into the impact of trust and gender on the adoption of mobile money in Zambia by utilizing the Technology Acceptance Model. Despite the limited body of research on mobile money, the author highlights the presence of cybersecurity challenges in this realm. In particular, the author draws attention to instances of impersonation attacks directed at the Zoono mobile money platform, where perpetrators pose as staff members to illicitly request PINs and access users' funds. Additionally, the study acknowledges the efforts of ZICTA, Airtel, and MTN in combating these specific cybercrimes. However, it's

worth noting that the most prevalent types of mobile phone-related cyberattacks, including phishing, SMishing, and Vishing, remain unaddressed thus the development of a Smishing detection model is vital.

This study emphasizes the importance of creating detection systems for less-represented languages in the field of cybersecurity. It recognizes that, in our interconnected world, digital communication spans linguistic boundaries. Neglecting the development of security measures for these languages leaves smaller linguistic communities vulnerable to cyber threats. The study argues that building detection systems for low-represented languages is essential to protect the security and privacy of users worldwide. According to (“Language Data for Zambia,” n.d.), the 2010 census in Zambia identified the most commonly spoken languages in Zambia, as per the census, are Bemba (35% of the population), Nyanja or Chewa (20%), Tonga (12%), and Lozi (6%). The proposed model aims to protect mobile money users from the financial losses they experience due to social engineering attacks that persistently exploit lesser-studied local languages and thus preventing financial losses due to smishing attacks can have a positive economic impact on individuals and businesses by safeguarding their resources and assets.

The study aims to address the increasing threat of smishing attacks by developing an Smishing Detection Model to classify Bemba and English Smishing text messages targeting mobile money users. This model utilizes Natural Language Processing (NLP) and Machine Learning to enhance the security of mobile money transactions. The goal is to effectively detect smishing attacks, thus providing protection against potential financial losses and safeguarding personal data from breaches. Furthermore, this study can contribute to the academic field by advancing the understanding of language-specific smishing detection, offering insights that may be useful for future research in cybersecurity and linguistics.

1.8 Preliminary sections of the project report

The rest of the project report is structured as follows: The second chapter will discuss the literature review. The third chapter will elaborate on methods used in the research. The fourth chapter looks at data, experiments, and implementation. The fifth chapter will discuss the results of the research. Lastly, sixth chapter will provide a summary of the research and conclude.

CHAPTER 2: LITERATURE REVIEW

2.1 General Background

The last two decades have witnessed a significant growth of mobile financial services on a global scale. In more advanced economies, the progress of mobile money services has been facilitated by swift technological advancements according to (Domfeh, 2018). According to the 2019 edition of the GSMA Mobile Money Metrics report, the East Asia & Pacific region boasted the highest count of active mobile money services among all continents. In Africa, particularly in sub-Saharan Africa, the advancement of mobile financial services has been greatly facilitated by the concerted effort to enhance financial inclusion. Over the past decade, mobile money services in Africa have experienced rapid growth, playing a pivotal role in expanding access to financial services for a significant portion of the population that lacks access to the conventional banking system. Following the introduction of M-PESA in Kenya in 2007, several other African nations, Zambia included, have adopted and integrated mobile money technologies.

As of the last quarter (Q4) of 2022, according to ZICTA statistics (ZICTA 2023), the number of active mobile phone subscribers stood at 19.6 million against a population of about 19.8 million. The diagram in Figure 2.1 shows the trend:

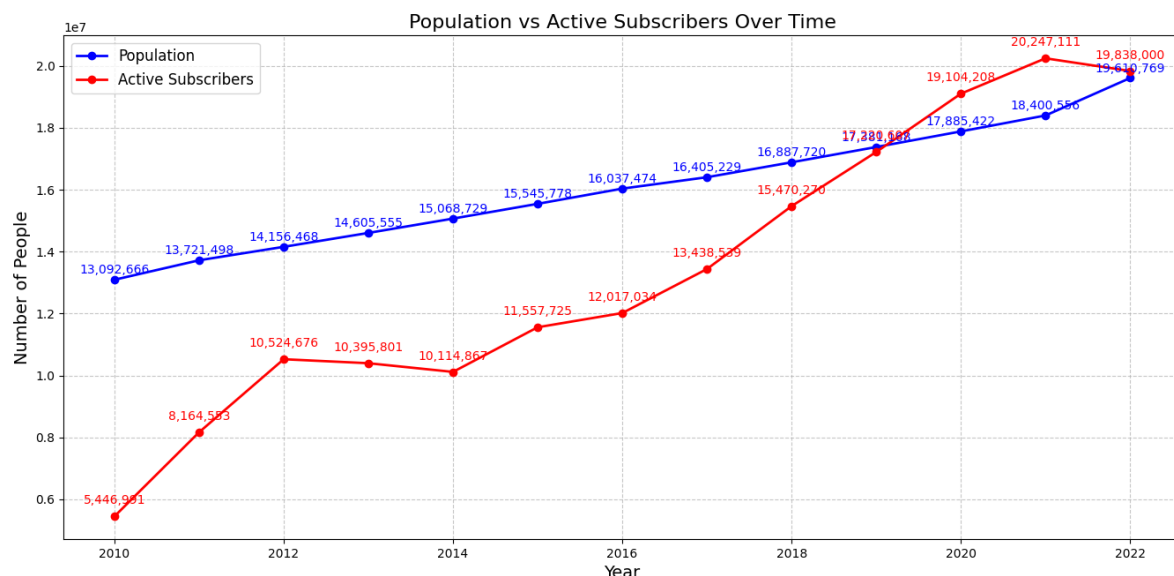


Figure 2.1 Population vs Active Subscribers (Zicta, 2023)

SMiShing is a variant of phishing that employs text messages sent via mobile phones and smartphones as its primary mode of operation. Smishing is a blend of 'SMS' (Short Message

Service) and 'phishing,' where the perpetrator employs text messaging as the medium of choice, as opposed to email (Mishra & Soni, 2019). As per CallHub, text messages enjoy a considerably greater response rate when compared to email (CallHub, 2016). In accordance with Delany, Buckley, and Greene (2012), this incentivizes malicious actors to opt for text messages as a communication medium with users. The cost-efficiency of this approach enables them to distribute a substantial volume of messages to users through a single SMS package (Delany, Buckley, & Greene, 2012).

2.2 Broad literature review of the topic

Current economies are largely driven by digital currency, and the widespread utilization of mobile devices has ushered in a novel market for digital financial services in developing nations. (Castle et al., 2016). Financial services for individuals who do not have access to traditional banking, like Mobile Money Services (MMS), typically operate through smartphone applications supported by mobile operators or banks. As the adoption of mobile money continues to rise, criminals are increasingly targeting this emerging avenue for financial transactions (Buku & Mazer, 2017; Pallangyo, 2022).

Smishing refers to a form of phishing conducted via text messages, where a malicious actor deceives the recipient by sending a text with the intention of fraudulently obtaining the recipient's sensitive information for financial gain, all while posing as a reliable source. Through smishing, harmful code can infiltrate mobile devices. Attackers have now shifted their attention towards mobile users for a number of reasons. The primary reason is the widespread use of smartphones, followed by the increasing reliance of users on mobile applications for various tasks. Additionally, many users mistakenly believe that two-factor authentication ensures that only trusted messages will reach their devices ("The Social Engineering Framework," 2017).

Throughout the years, mobile service providers have attempted multiple methods to identify harmful text messages, achieving limited success in their efforts. As an example, Jain and Gupta (Jain & Gupta, 2018) utilize a rule-based technique that applies a predefined set of rules to evaluate each SMS passing through an SMS gateway. The use of blacklist and whitelist methods has proven ineffective, as attackers frequently change their mobile numbers, rendering these techniques futile.

2.3 Critical review of related works

Throughout the years, the field of Smishing detection has predominantly relied on a combination of methods such as blacklisting, heuristics, and visual analytics. These techniques have formed the cornerstone of efforts to identify and mitigate Smishing threats in various communication systems and digital platforms. Numerous approaches have been suggested for identifying Smishing attacks; however, perpetrators have managed to exploit weaknesses in current solutions and have devised techniques that can circumvent security measures. For instance, a rule-based method by Jain and Gupta (Jain & Gupta, 2018) employs a set of rules against every SMS going through an SMS gateway. Blacklist and whitelist techniques have also been employed to no avail, because attackers keep on changing mobile numbers every now and then. In addition, Jain and Gupta (Jain & Gupta, 2019) introduce a method for detecting Smishing messages based on a feature-based approach. They identify ten distinct features that can differentiate Smishing messages from genuine ones. Among these, two features are encoded as '0' for legitimate messages and '1' for Smishing messages, while the other two features primarily represent legitimate messages, and the remaining eight are indicative of Smishing messages. Following experimentation, the classifier achieved impressive performance metrics, with a true positive rate of 94.2%, a true negative rate of 99.08%, and an overall detection accuracy of 98.74%.

(Joo et al., 2017) introduced a system called 'S-Detector' designed to identify Smishing attacks. The S-Detector comprises four main components: an SMS monitor, SMS analyzer, SMS determinant, and Database. It evaluates both the URL and the content of text messages. To differentiate Smishing messages from legitimate ones, the authors employed a Naïve Bayesian Classifier, identifying the words that are more commonly used in Smishing messages.

In their comprehensive investigation aimed at shedding light on spear phishing attacks, (Liu et al., 2021) devised and put into practice a natural language processing (NLP) detection algorithm to identify SMS spear phishing attacks. Their collaboration with 360-mobile-safe, a prominent security vendor in China, facilitated the creation of a substantial dataset comprising 31 million real-world spam messages associated with spear phishing. Following data preprocessing, two distinct vectorization techniques, Word2Vec and TFIDF, were employed. The study analyzed 10,399 consistently labeled messages and tested various conventional machine-learning classifiers. The combination of Logistic Regression and Word2Vec emerged as the most effective, achieving an impressive average F1-Score of 93.41%.

A Naïve-Bayes algorithm was employed by (Kipkebut et al., 2019) to classify spam communications directed towards Kenyan mobile money customers. The study gathered English-language spam mails and conducted experiments using the Weka toolbox. Through trial and error, they were able to achieve 96.1039% accuracy.

(Mishra & Soni, 2021) introduce a prototype system that employs the Backpropagation Algorithm and conducts a comparative analysis with three conventional classifiers. The prototype system comprises two key phases: a domain checking phase and an SMS classification phase. To assess the effectiveness of these classifiers, a dataset consisting of 5,858 messages was utilized. The classifiers tested included Random Forest, Decision Tree, Naïve-Bayes, and the Backpropagation Algorithm. Notably, the Backpropagation Algorithm outperformed the other classifiers, achieving an impressive accuracy rate of 97.93%.

(Nturibi, 2018) presented a framework designed to identify Smishing and vishing attacks associated with mobile money transactions. This framework outlines recommended actions for customers when confronted with these types of attacks

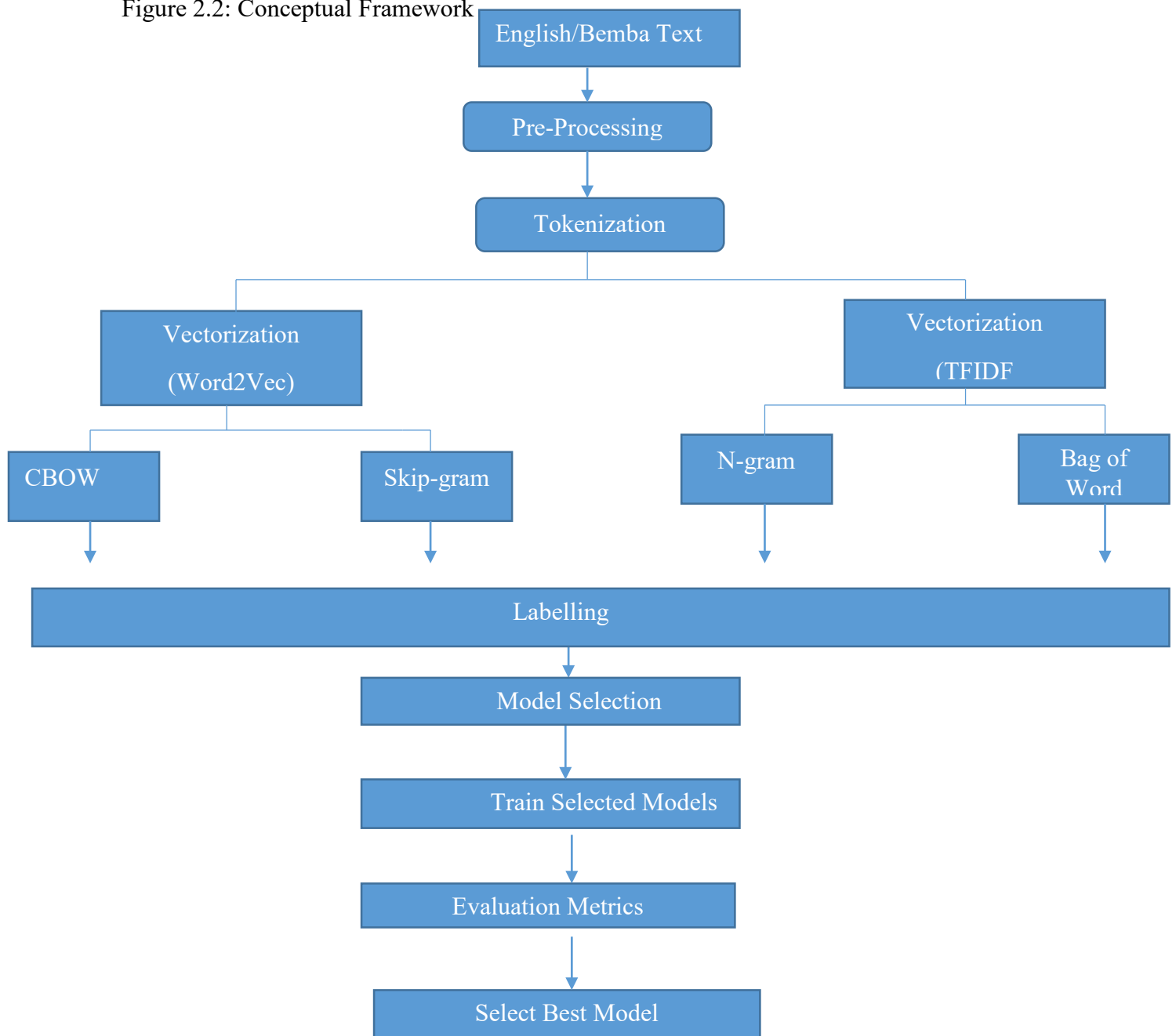
(Chen, Yan, Zhang, & Kantola, 2015) introduced a Smishing management system that relied on trust management principles. This system's objective was to regulate or screen Smishing attempts by assessing the trust relationships established between message senders and recipient

(Foozy, Ahmad, & Abdollah, 2013) used a classification method for detecting phishing on mobile devices. This encompassed various types of mobile device phishing, such as Bluetooth phishing, SMS phishing, voice phishing, and mobile web application phishing. Furthermore, the researchers introduced and conducted comparisons of technologies designed for detecting mobile device phishing.

2.4 Conceptual framework/Theoretical framework

The study's primary goal is to create an effective Smishing detection model using natural language processing (NLP) and machine learning (ML) techniques. Key motivations for choosing machine learning over deep learning include the reduced resource demands of machine learning models (Xin et al., 2019). Smishing messages exhibit distinct linguistic patterns and typically include mobile numbers for fraudulent transactions. The proposed model's architecture, as outlined in Figure 2.2 encompasses data collection (English and Bemba text), preprocessing (including stopword removal and tokenization), and word vectorization using both Word2vec and TF-IDF vectorization techniques. Feature selection and parameter tuning enhance model training, which is carried out using the "Bag of Words" (BoW) and n-gram approaches. N-grams, in the form of 2-5 sequences of words, are used to explore contextual relationships and identify the best-performing model. Figure 2.2 shows the conceptual framework of the model.

Figure 2.2: Conceptual Framework



2.5 Proposed model/system

The proposed model aims to enhance smishing (SMS phishing) detection by leveraging the strengths of both Random Forest and Naïve Bayesian algorithms. Smishing involves deceptive text messages sent to trick individuals into revealing sensitive information, and the model targets both Bemba and English languages.

The proposed model is a hybrid approach for detecting smishing (SMS phishing) in both Bemba and English languages. It combines the strengths of Random Forest and Naïve Bayesian algorithms, utilizing natural language processing (NLP) and machine learning. The model aims to address the nature of smishing and employs evaluation metrics such as Matthews Correlation Coefficient, Precision, Recall, F1-score, and Accuracy for comprehensive performance assessment.

- *Matthews Correlation Coefficient (MCC)*: A measure of the quality of binary classifications, considering true and false positives and negatives.
- *Precision*: Ratio of true positive predictions to the total positive predictions, measuring accuracy among positive predictions.
- *Recall*: Ratio of true positive predictions to the total actual positives, indicating the model's ability to capture all relevant instances.
- *F1-score*: The harmonic mean of precision and recall, providing a balanced measure of model performance.
- *Accuracy*: Overall correctness of the model's predictions.

2.6 Comparison with related works

Table 2.1 Comparison with related works

Attribute/Work	Classifier	Domain	Language	Modelling Approach	Evaluation Metrics
Joo et al. (2017)	Naïve Bayesian	Smishing	English	Machine Learning	Accuracy
Liu et al. (2021)	Logistic Regression	Smishing	English	Natural Language Processing	Precision, Recall, False Negative, False Positive and F1-Score

Mishra & Soni(2021)	Backpropagation	Smishing	English	Deep Learning	Accuracy, Area Under the Curve & Execution Time
Kipkebut et al. (2019)	Naïve Bayesian	Smishing	English	Machine Learning	Precision, Recall, Accuracy, True Positive, False Negative, True Negative and False Negative-Rates
(Mambina, Ndibwile, & Michael, 2022)	Random Forest	Smishing	Swahili	Machine Learning	Log-Loss, Area Under the Curve & Execution time
Proposed Model	Random Forest & Naïve Bayesian	Smishing	Bemba and English	Natural Language Processing and Machine Learning	Matthews Correlation Coefficient, Precision, Recall, F1-score

CHAPTER 3: METHODOLOGY

In this section, the research methodology of the study is presented which essentially outlines the sequence through which the study was carried out: Research design, Adopted method and justification, Association of Methods to Project and Research Data and Datasets:

3.1 Research Design

In this study, a hybrid descriptive research design (Siedlecki 2020) is used and this approach involves employing diverse research methods and tools to explore an array of variables. Unlike experimental research, the aim isn't to manipulate or control variables; instead, it is focused on observing, discovering, and measuring different phenomena without intentional intervention. This enabled the research to gain a comprehensive understanding without influencing the natural course of events or factors under investigation.

The hybrid descriptive research design employed in this study facilitates a comprehensive and non-intrusive exploration of Smishing behaviours among mobile money users. This approach involves the use of diverse research methods and tools, such as natural language processing (NLP) and machine learning, to observe and measure various variables without artificial manipulation.

In the realm of cybersecurity, Smishing (SMS phishing) poses a significant threat to mobile money users, exploiting textual and behavioural cues to deceive individuals into disclosing sensitive information. Understanding the evolving nature of Smishing attacks requires a research approach that captures the natural course of events without intervention.

Through this observational nature, the research aims to comprehensively analyse linguistic nuances, and contextual information related to Smishing attempts. By integrating methods like NLP and machine learning, this approach enables the development of a detection model adaptable to dynamic changes in Smishing tactics. This adaptability ensures that the model reflects real-world scenarios and enhances its accuracy in identifying Smishing attempts among mobile money users.

3.2. Adopted Method and Justification

The chosen approach involves the integration of Natural Language Processing (NLP) techniques and Machine Learning (ML) models to create a robust Smishing detection system

tailored for mobile money transactions of which an Android Application is integrated. This methodology hinges on the synergy between NLP algorithms designed for text analysis such as and a suite of ML algorithms, including but not limited to Naive Bayes, Random Forest, and Logistic Regression.

The rationale behind this method selection lies in the demonstrated effectiveness of these algorithms in handling unstructured text data, a common format in Smishing attempts. NLP algorithms play a pivotal role in deciphering the nuances of textual content, while ML models like Naive Bayes, Random Forest, and Logistic Regression excel in identifying intricate patterns within the vast and dynamic landscape of mobile money transactions.

By leveraging these established methodologies, the research aims to develop a comprehensive and adaptable Smishing detection model capable of navigating the intricate and ever-evolving nature of fraudulent activities within the realm of mobile money.

3.3 Association Of Methods To Project

The chosen methodologies offer a direct pathway to analyse textual content sourced from SMS messages and transaction logs. Through the strategic application of Natural Language Processing (NLP), these NLP methods empower the extraction of deeper semantic meanings embedded within the text. Simultaneously, they facilitate the detection of suspicious Smishing patterns that might otherwise remain concealed.

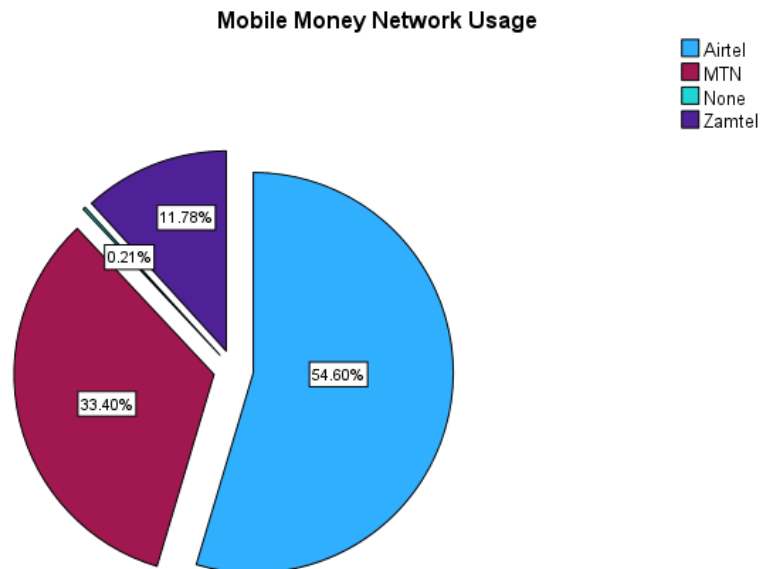
Moreover, the integration of Machine Learning (ML) models within these methodologies plays a pivotal role. These models have been trained to detect patterns and features, enabling the classification of incoming messages into two distinct categories: legitimate messages (Non-Smishing) and Smishing (Smishing) attempts. By leveraging learned features and patterns, these ML models efficiently categorize and differentiate between safe (Non-Smishing) and suspicious messages (Non-Smishing), contributing significantly to the safety of mobile money users.

4.4 Research Data And Datasets:

The approach has revolved around leveraging diverse and substantial datasets. One of my primary tools for data collection has been Google Forms, an online survey through which both qualitative and quantitative data were collected and later analysed using SPSS. The results are shown below.

Survey Question: Which Mobile Money Network do you use?

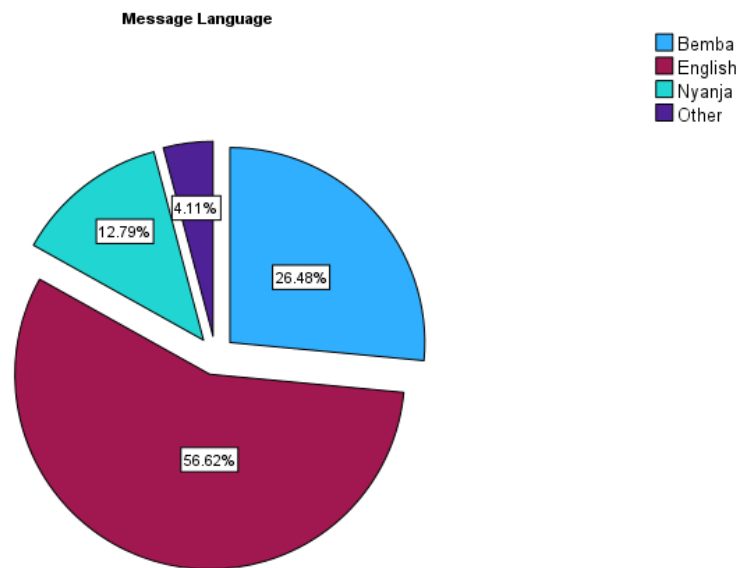
Fig 3.1 Mobile Money Network Usage



In Fig 3.1, Airtel has the highest usage frequency at 255, accounting for 54.6% of the total usage. This indicates that Airtel is the most commonly used network among the surveyed population. MTN follows Airtel with a usage frequency of 156, representing 33.4% of the total usage. While it's notably lower than Airtel, it still holds a significant portion of the market share. There's a category labelled "None" with just 1 entry, which represents 0.2% of the usage. This could potentially indicate respondents who aren't using any of the listed networks. Zamtel has a usage frequency of 55, making up 11.8% of the total usage. While it's the smallest portion among the listed providers, it still holds a notable share of the market.

Survey Question: In what language was the text?

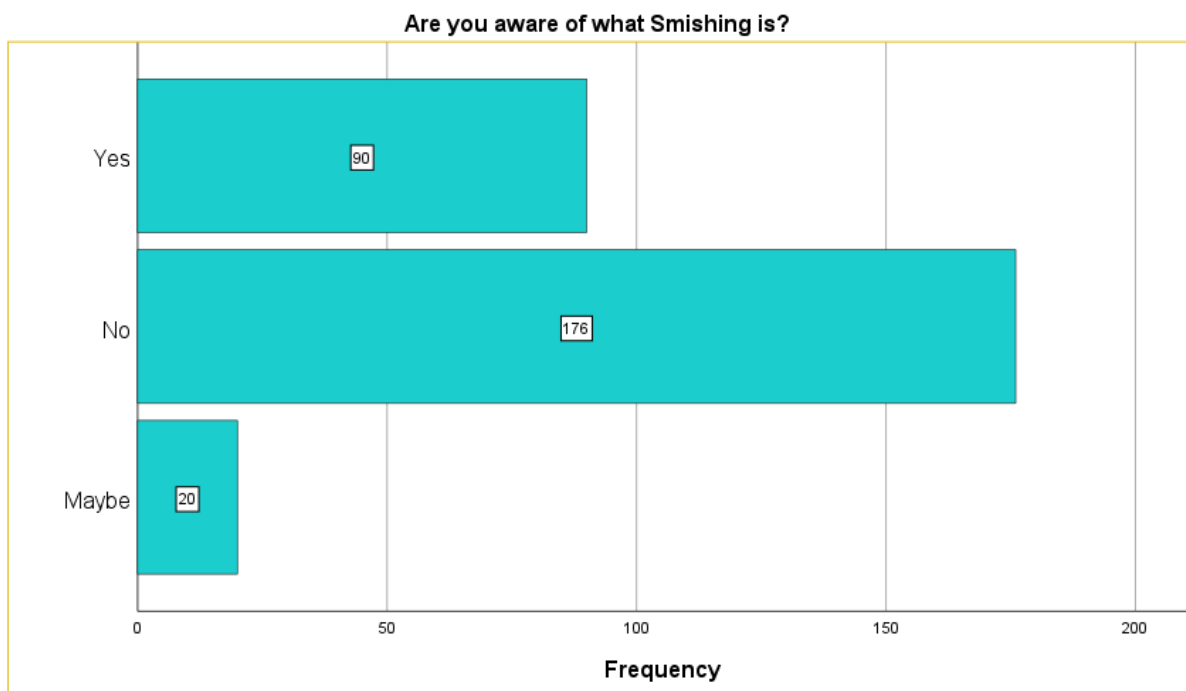
Fig 3.2 Message Language



- In Fig 3.2 English stands out as the most frequently used language, with a frequency of 124 instances, representing 56.6% of the total language usage. This suggests that English is the predominant language among the surveyed population, occupying a significant majority. Bemba follows with a frequency of 58, constituting 26.5% of the language usage. While it's notably lower than English, it still represents a substantial portion of the surveyed population. Bemba is the second most commonly spoken language among the respondents. Nyanja has a usage frequency of 28, making up 12.8% of the language usage. It holds a smaller but still notable presence among the surveyed population. The "Other" category comprises 9 instances, representing 4.1% of the language usage..

Survey Question: Are you aware of what Smishing is?

Fig 3.3 Smishing Awareness



The results in fig 3.3 are analysed as follows:

- **Yes:** 90 respondents, representing 31.5% of the total responses, indicated that they are aware of what smishing is. This group likely has an understanding of the term and its implications, suggesting a certain level of familiarity with this form of cyber threat.
- **No:** A majority of respondents, 176 individuals constituting 61.5% of the total responses, stated that they are not aware of what smishing entails. This group lacks knowledge or awareness regarding smishing, indicating a potential lack of familiarity with this specific type of cyber-attack.
- **Maybe:** A smaller subset of respondents, 20 individuals representing 7.0% of the responses, indicated uncertainty regarding their awareness of smishing. This group might have heard the term but might not possess a clear understanding of its meaning or context.

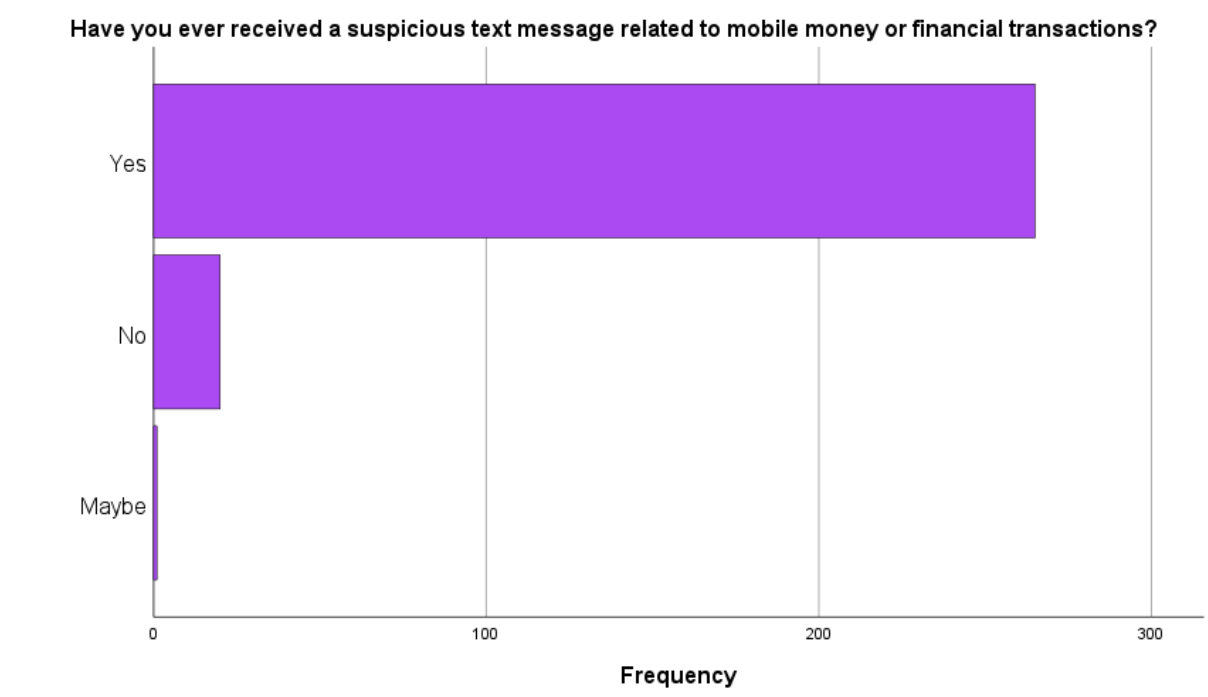
This shows that a significant portion of the surveyed population lacks awareness of smishing, while a minority are familiar with it. Understanding the level of awareness among the

population is crucial for cybersecurity awareness campaigns aimed at mitigating the risks associated with smishing attacks. Efforts to increase awareness and educate individuals about smishing could be essential in enhancing overall cybersecurity preparedness.

Survey Question: Have you ever received a suspicious text message related to mobile money or financial transactions?

:

F.g 3.4 Number of Received Suspicious Message



The results in fig 3.4 are analysed as follows:

- **Yes:** A significant majority of respondents, 265 individuals, accounting for 92.7% of the total responses, reported that they have received suspicious text messages related to mobile money or financial transactions. This high percentage indicates a prevalent occurrence of such messages within the surveyed population, highlighting a notable exposure to potential smishing attempts or fraudulent activities targeting financial transactions.
- **No:** Only 20 respondents, constituting 7.0% of the responses, stated that they have not received any suspicious text messages related to mobile money or financial

transactions. This group represents a minority within the surveyed population, suggesting that the majority have encountered or been targeted by these types of messages.

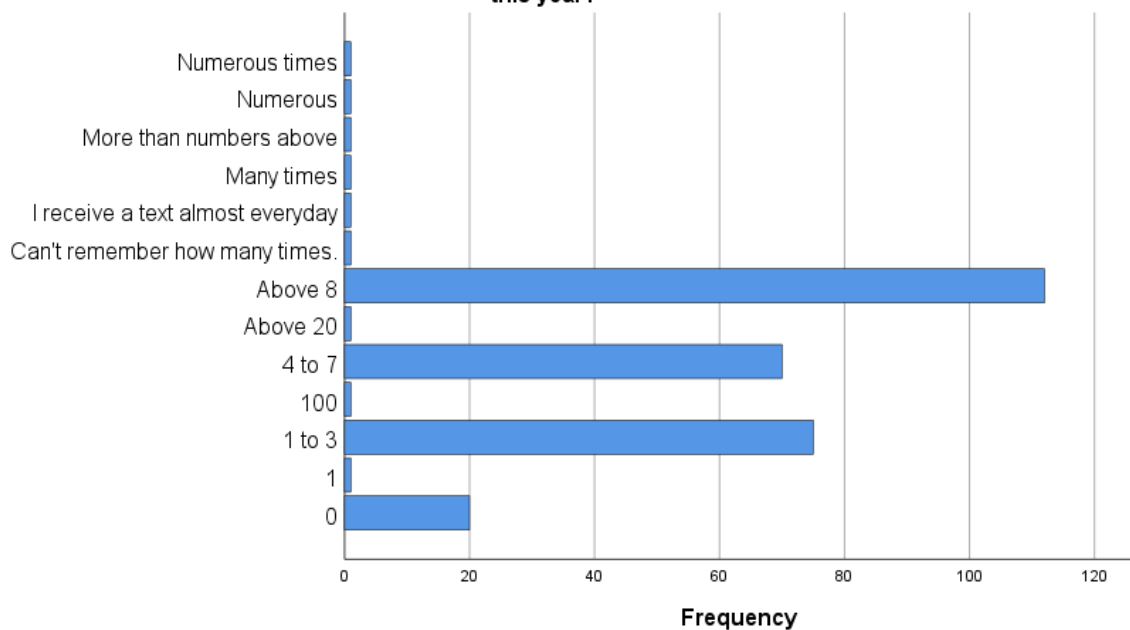
- **Maybe:** A single respondent, representing 0.3% of the responses, expressed uncertainty about whether they had received suspicious text messages related to mobile money or financial transactions. This response indicates a very small segment of the population that is unsure about their exposure to such messages.

This emphasizes a prevalent exposure to suspicious text messages concerning mobile money or financial transactions among the surveyed population. The overwhelming majority have encountered these messages, signifying a potentially widespread issue that requires attention and awareness campaigns to educate individuals about identifying and avoiding such fraudulent attempts.

Survey Question: How Many times have you received suspicious text message related to mobile money or financial transactions this year?

F.g 3.5

How many times have you received suspicious text message related to mobile money or financial transactions this year?



The Captured responses in fig 3.5 regarding the frequency of receiving suspicious text messages related to mobile money or financial transactions over the course of a year indicate:

- **0:** 20 respondents (7.0%) reported receiving no suspicious text messages related to mobile money or financial transactions throughout the year.
- **1:** A single respondent (.3%) indicated receiving such a message once during the year.
- **1 to 3:** 75 respondents (26.2%) received suspicious texts between 1 to 3 times within the year, signifying a moderate but relatively infrequent occurrence.
- **4 to 7:** 70 respondents (24.5%) encountered these messages between 4 to 7 times over the year, indicating a somewhat higher frequency compared to the previous category.
- **Above 8:** 112 respondents (39.2%) reported receiving these messages more than 8 times during the year, representing a substantial portion of the surveyed population experiencing these messages frequently.
- **100, Above 20, Can't remember how many times., I receive a text almost every day, Many times, More than numbers above, Numerous, Numerous times:** Each of these categories had one respondent (.3% each), representing various responses indicating a high frequency or uncertainty about the exact count of received suspicious texts. These responses collectively account for the remaining 2.1%.

This demonstrates a wide range of experiences within the surveyed population regarding the frequency of receiving suspicious text messages related to mobile money or financial transactions. While some individuals rarely received such messages or couldn't recall the frequency accurately, a significant portion encountered them frequently, with a notable number reporting a high frequency of occurrences, potentially indicating a persistent issue of smishing attempts or fraudulent messages targeting financial transactions.

Complementing this is the labelled dataset, a cornerstone of the research. It contains confirmed Smishing messages as well as non-Smishing ones. This dataset serves as the backbone for training and validating models and algorithms aimed at detecting between malicious Smishing attempts and legitimate messages. It's a critical piece to develop effective strategies to detect Smishing. The tables (table and table) shows the first 5 rows of the Smishing English Data Set and the Smishing Bemba Data Set respectively.

Table 3.1 English Smishing Dataset

Label	Text
Smishing	Smishing, Yes phiri am bwana Anold. tell your son to bring the school document to my office they is a space for ZAF and Zambia Army whatsapp line 0975800697
Smishing	Smishing, I'm requesting you to send that money in airtel agent 0979611332 Name is coming Simanyika maybin. My number of mtn is not working. thanks
Smishing	To send that money use this number of Airtel 0978329692 the name will come Edward Sichula. my number is not working in Airtel money. Thanks
Smishing	Please call me now. The money for CDF and youth empowerment is out's
Smishing	Ok use this airtel number to send that money name will come Joyce. My number is not working in mobile money

Table 3.2 Bemba Smishing Dataset

Label	Text
Smishing	Please call me now. mupoke indalama sha C.D.F ishabalanda naba youth. tumeni NRC registration number mupoke indalama shenu.
Smishing	indalama sha cdf na youth empowerment nashifuma tumeni NRC number yenu mupokeko ulupiya. Tumeni phone.
Smishing	Natukwata gold amasaka yabili tuleshitisha tumeni indalama
Smishing	Natukwatako emalod na gold tuleshitisha mgakuli abengafwaya. Please call me. Nine Kataso.
Smishing	Ulupiya lwaba Youth empowerment nalufuma tumeni NRC number yenu temuni mupoke ulupiya lwenu

CHAPTER 4: DATA, EXPERIMENTS AND IMPLEMENTATION

This section describes the prototype of the proposed system. The implementation environment of the prototype is running as an Android emulator on Android OS Ver 9.0. The prototype was implemented on the basis of the scenario of responding to Smishing attack in an Android environment. Simulation of sending of the messages to the android was done using telnet and connecting to the Android App.

4.1 Appropriate Modeling In Relation To Project

Specific algorithms were chosen considering their suitability for NLP and machine learning tasks.

Chosen Algorithms and Explanation: Random Forest, Naive Bayes And Logistic Regression: These were selected due to their effectiveness in analysing text and classifying data. For instance, Random Forest is an ensemble learning method suitable for text-based features, while Naive Bayes and Logistic Regression are good choices for classification tasks.

Random Forest: This ensemble learning method is well-suited for analysing text-based features. It's effective in handling complex interactions among features, which can be beneficial in NLP tasks.

Suitability for NLP:

- In the context of smishing detection, where the analysis of text messages or transaction descriptions is essential, Random Forest's ability to capture intricate relationships among words and features is advantageous.
- Handling Language Features: Random Forest, being adept at handling text-based features, can analyse Bemba messages by converting them into numerical representations using techniques like TF-IDF or word embedding's specifically tailored for the Bemba language. In this research, TFIDF is used.
- Complex Interactions in Bemba: It can capture complex relationships among words or phrases in Bemba messages, aiding in detecting smishing attempts even within a different language context.

Naive Bayes: Known for its simplicity and efficiency, Naive Bayes works well with text data. Despite its "naive" assumption of feature independence, it often performs admirably in classification tasks, especially in NLP applications.

Suitability for NLP:

- For smishing detection, Naive Bayes can effectively handle textual data, making predictions based on word occurrences or other text-related features, contributing to the identification of suspicious transactions.

Naive Bayes, despite its independence assumption, can work reasonably well with Bemba text data. It relies on word occurrences or frequencies, making it adaptable for Bemba messages once they're suitably encoded into numerical representations.

Logistic Regression: This linear model is commonly used for classification tasks. It's particularly effective when the relationship between the features and the target variable is linear, making it a reliable choice for certain NLP scenarios.

Suitability for NLP:

Linear Representation: Logistic Regression's strength lies in linear representation. If relationships between features and the target variable in Bemba messages exhibit linear tendencies, Logistic Regression can still be effective.

Rationalization for the Selection:

- **Textual Data Emphasis:** All three algorithms were chosen due to their compatibility and effectiveness in handling textual data, which is prevalent in smishing detection tasks involving transaction descriptions or message content.
- **Diverse Model Characteristics:** Each algorithm brings distinct strengths to the table: Random Forest for handling complex interactions, Naive Bayes for its simplicity and efficiency, and Logistic Regression for linear relationship representation. This diversity can contribute to a more robust ensemble or comparative analysis for smishing detection.

By leveraging these algorithms' strengths in handling text-based features and their varying capabilities in understanding the textual content of mobile money transactions, the overall detection system can benefit from a more comprehensive analysis and interpretation of Smishing patterns within the data.

4.2 Techniques, Algorithms, Mechanisms

Natural Language Processing Techniques in the Prototype:

1. **Tokenization:** This process involves breaking down text into individual words or tokens. In the Prototype, it's achieved using **word_tokenize** from NLTK.
2. **Stopwords Removal:** Common words like 'fye', 'bonse', 'shani', 'kuli', 'fyonse etc., which carry little semantic meaning, are eliminated using a predefined set of Stopwords from NLTK's corpus.
1. **Stemming:** Reducing words to their base or root form to normalize the text. The algorithm uses the SnowballStemmer to perform stemming.

Feature Engineering:

The prototype uses TF-IDF (Term Frequency-Inverse Document Frequency) for feature extraction. This involves:

- **TF-IDF Vectorization:** Converts text data into numerical vectors. The **TfidfVectorizer** from Scikit-learn is utilized with specific configurations (ngram_range, min_df, and max_features) to transform the text into a format suitable for machine learning algorithms.

Feature Selection Methods:

The target column was encoded into “Non-Smishing” and “Smishing”, where all legitimate messages were encoded with label “Non-Smishing” and all Smishing messages were encoded with label “Smishing”. Furthermore, it implicitly performs feature selection by setting **max_features** in **TfidfVectorizer** to limit the number of features.

Machine Learning Algorithms (Random Forest Classifier used as an Example):

1. **Random Forest Classifier:** Employed to learn patterns from the TF-IDF transformed text data. The **RandomForestClassifier** is used, and hyper parameter tuning is done using **GridSearchCV** to optimize its performance.
2. **Handling Imbalanced Classes:** Addressing the skewed distribution between smishing and non-smishing texts is done using Synthetic Minority Over-sampling

Technique (SMOTE) from imbalanced-learn. However, the Bemba dataset is currently balanced.

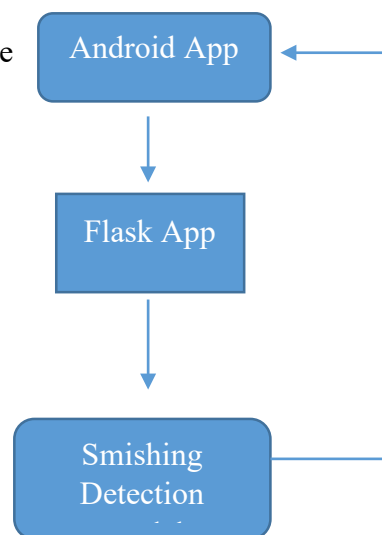
4.3 Implementation:

In this section, the architecture and flowchart of the proposed framework is discussed.

ARCHITECTURE

The proposed Smishing Architecture is comprised of an Android Application, Flask App and Smishing Detection Model as shown in Fig 4.1. The Android App consists of SMS Monitor, Text field, HTTP Post Module and a Response feedback. SMS monitor, actively monitors SMS Activities and of the Smartphone and upon receiving a message, the message is inserted in the Text field and sent to a Flask API through an HTTP Post Request. The App actively waits for a response from the Flask API and once a response is received, a Response is displayed. The smishing detection model architecture currently detects the type of mobile money message whether it is Smishing or Non-Smishing by firstly pre-processing the text, dataset normalization by using SMOTE and classification using classifiers like Random Forest algorithm.

Fig 4.1 Smishing Architecture



FLOWCHARTS

The model has been integrated with an Android Application. The Integrated architecture consists of an Android Application, Flask App and the trained Model.

SMISHING DETECTION

This subsection looks at how the Smishing detection is carried out by the model and fig 4.2 is a flowchart of the Smishing detection process.

1. Text Pre-processing:

- This step involves cleaning and preparing the text data for analysis. It includes:
 - **Lowercasing:** Converting all text to lowercase to ensure uniformity.
 - **Removing Punctuation:** Eliminating non-alphanumeric characters that don't contribute to the meaning.
 - **Removing Stopwords:** Common words (like "the," "and," "is") that don't add much value to the analysis for English and common words like ('fye', 'bonse', 'shani', 'kuli', 'fyonse) for Bemba
 - **Stemming/Lemmatization:** Reducing words to their root form to normalize variations (e.g., "running" becomes "run").
 - **Handling Special Characters or Numbers:** Dealing with specific patterns like URLs, numbers, or emojis based on the task.

2. Tokenization (TF-IDF Vectorizer):

- Tokenization breaks text into smaller units like words, phrases, or characters (tokens) for analysis.
- TF-IDF (Term Frequency-Inverse Document Frequency) Vectorizer converts text into numerical vectors. It represents each document (piece of text) as a vector where each feature represents the importance of a term in that document relative to a collection of documents.

- TF-IDF weighs terms based on their frequency in a document against their occurrence in the entire corpus, emphasizing terms that are more specific to a document.

3. Dataset Normalization:

- Normalizing data ensures that features are on a similar scale and don't skew the model's learning process.
- For text data, normalization might involve scaling the TF-IDF vectors or any other feature engineering necessary for the chosen model.

4. Train Selected Model:

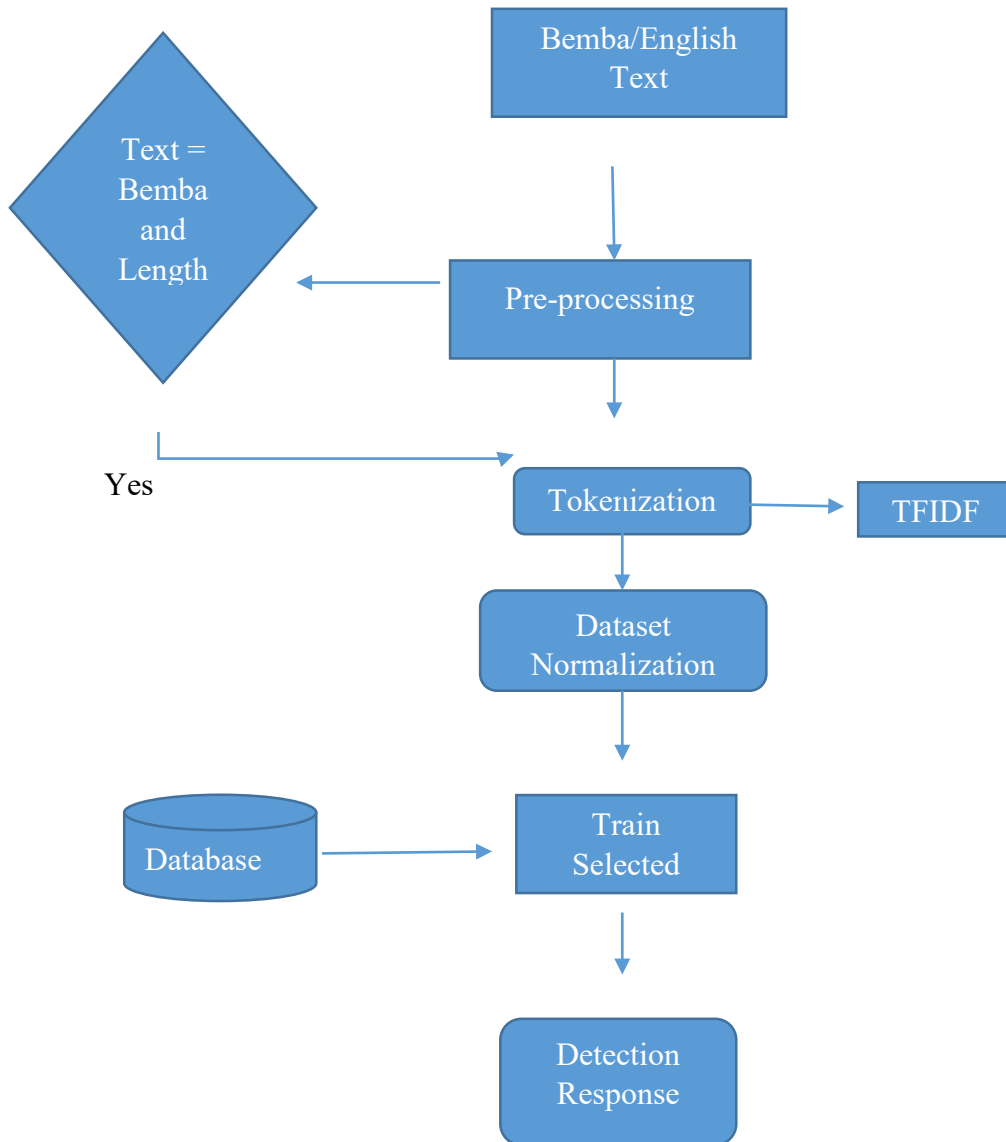
- Once the data is pre-processed and prepared, it's split into training and testing sets.
- A machine learning model (e.g., Random Forests, Naïve Bayes) is used.
- The model is trained on the training data, where it learns patterns and relationships between the input (pre-processed text) and the output (labels).

5. Detection Response:

- After training, the model is tested on the unseen test data to evaluate its performance.
- For text classification tasks, such as sentiment analysis or spam detection, the model predicts the labels for the test text data.
- The response or output indicates the model's predictions, showing how accurately it can classify or detect patterns in new, unseen text data.

SMISHING DETECTION FLOWCHART

Fig 4.2 Smishing Detection Flowchart



Code Snippets

Snippet 1: Pre-Processing

```
def preprocess_bemba_text(text):
    text = re.sub( pattern: r'^A-Za-z', repl: ' ', text)
    tokens = word_tokenize(text.lower())
    tokens = [stemmer.stem(word) for word in tokens if word not in bemba_stopwords]
    return ' '.join(tokens)
```

```
def preprocess_bemba_dataset(data):
    data['clean_text'] = data['text'].apply(preprocess_bemba_text)
    return data
```

Snippet 2: Model loading and Smishing Detection


```
# Load the trained model and vectorizer
def load_model(model_file, vectorizer_file):
    model = joblib.load(model_file)
    vectorizer = joblib.load(vectorizer_file)
    return model, vectorizer

# Smishing detection
def detect_smishing(message, model, vectorizer):
    clean_message = preprocess_bemba_text(message)
    message_tfidf = vectorizer.transform([clean_message])
    prediction = model.predict(message_tfidf)
    return prediction[0]
```

Snippet 3: Message to be checked provided and detect_smishing function in Snippet 2 called.

```
message_to_check = "Indalama shabalana nashifuma, tumeni NRC number yenu"
result = detect_smishing(message_to_check, model, tfidf_vectorizer)
```

Snippet 4: Result

 The message is identified as smishing.

Snippet 5: Model loading Training on English Dataset

```
def load_or_train_model(file_path):
    input_hash = calculate_hash(file_path)

    if input_hash == get_cached_input_hash():
        return load_cached_model()

    model = api.load("word2vec-google-news-300")
    data = pd.read_csv(file_path)
    data['processed_text'] = Parallel(n_jobs=-1)(delayed(preprocess_text)(text) for text in data['text'])

def vectorize_text(text):
    word_vectorized = np.array([model[word] for word in text if word in model], dtype=np.float32)
```

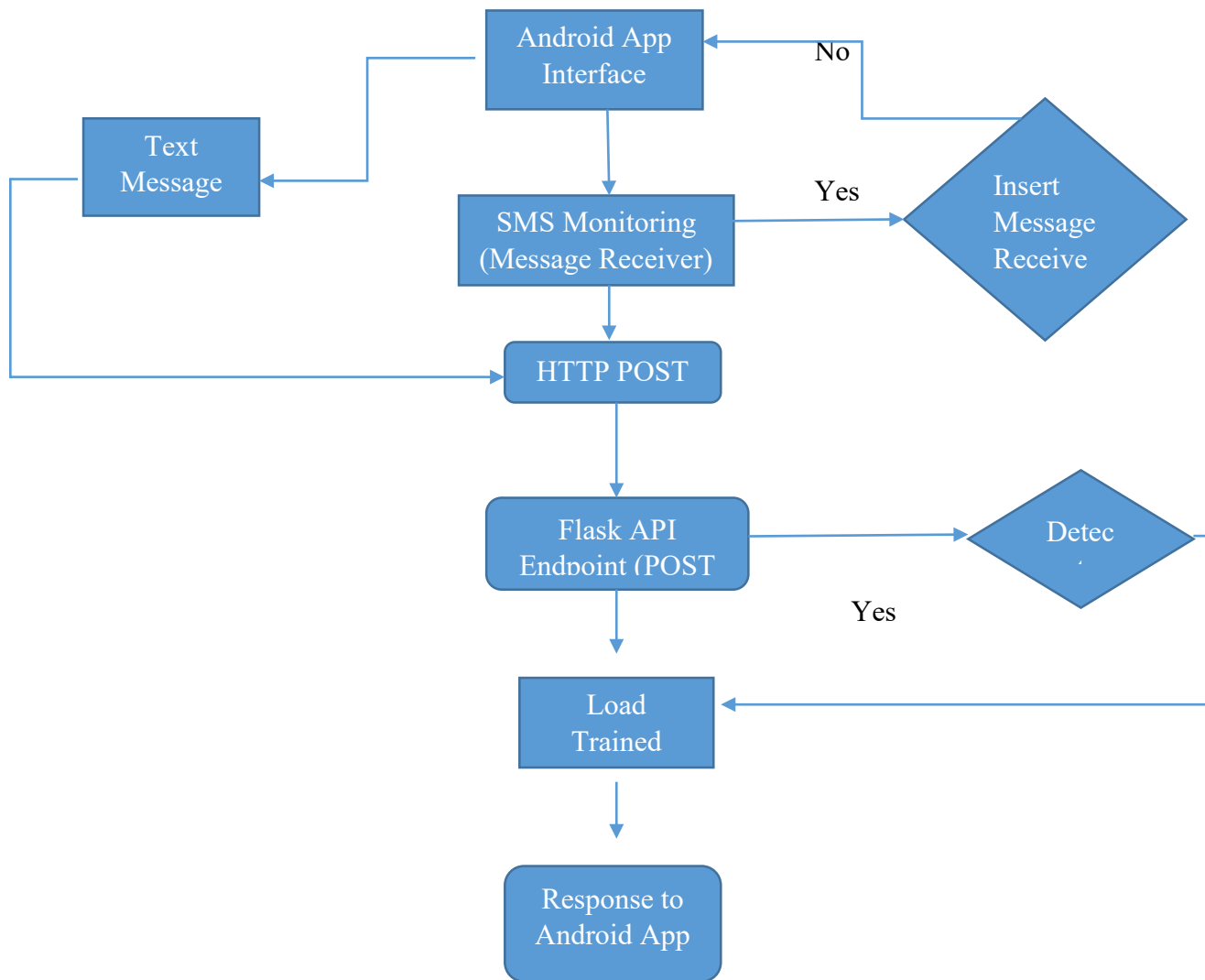
ANDRIOD APP INTEGRATION

In this subsection, the proposed prototype of the Smishing Detection using an Android is described and illustrated with a flowchart fig 4.3. The Android app acts as the primary interface for users to interact with the smishing detection model. Its role revolves around several key functions:

1. **User Alerts and Notifications:** The app serves as a means to alert users about potential smishing attempts. It notifies them when a suspicious message is received.
2. **Real-time Monitoring:** It constantly monitors incoming messages, analysing their content and to identify potential smishing messages.
3. **Integration with Messaging Services:** It seamlessly integrates with the device's messaging services, allowing users to continue using their preferred messaging app while the smishing detection system operates in the background.

ANDRIOD APP INTEGRATION FLOWCHART

Fig 4.3 Android App flowchart



1. **Receiver of Requests:** For the Android app to get to check if a text message is potentially a smishing attempt, it sends a request to the Flask app's designated endpoint (`/detect_smishing`) via an HTTP POST request of which a text message can be directly posted through a text field and the Android app is also actively listening for messages from the phone of which the apps gets the message that has been received and sends it to Flask.

2. **Processing the Request:** Upon receiving this request, the Flask app is called. It extracts the text message from the request body and prepares it for analysis.
3. **Communication with the Model:** The Flask app holds the key to the trained detection model. It uses this model, which has learned from previous examples, to analyse the message. This involves breaking down the message, removing unnecessary words, and transforming it into a format that the model can understand.
4. **Model's Verdict:** Once the message is in a suitable format, the Flask app passes it to the detection model for evaluation. The model uses its knowledge to predict whether the message is likely to be a smishing attempt or not.
5. **Response to the Android App:** The Flask app receives the result from the model. It then creates a response (typically in JSON format) containing the result. This response is sent back to the Android app that initiated the request.

The Flask app serves as a bridge between the Android app (which needs to detect smishing messages) and the trained detection model (which knows how to identify smishing). It works as follows:

1. **Flask API Endpoints:**

- The Flask app creates endpoints to handle incoming requests from the Android app.
- An endpoint **/detect_smishing** is established to receive text data for smishing detection.

2. **Request Handling:**

- When the Android app sends a POST request to **/detect_smishing** with the message data in the request body, Flask receives this request at the designated endpoint.

3. **Processing Requests:**

- The Flask backend retrieves the text data from the request body.
- It performs pre-processing tasks on the text data, such as tokenization, cleaning, and formatting, to prepare it for model prediction.

4. **Passing Data to the selected Model:**

- The pre-processed text is then passed to the selected loaded model for prediction.
- The Flask app sends the pre-processed text to the models e.g. Random Forest, Naive Bayes, and Logistic Regression models.

5. **Obtaining Prediction Results:**

- The model receives the pre-processed data and utilize their respective **predict()** methods to generate predictions for the given text.
- Each model generates a prediction result indicating whether the text is classified as smishing or not.

6. **Returning Results and Sending Response to Android App**

- The Flask backend collects the prediction results from the selected model.
- Finally, the Flask app constructs a response containing the prediction outcome or aggregated results in JSON format.
- This response is sent back to the Android app that initiated the request, enabling the user to receive the model's prediction regarding whether the text is Smishing or Non-Smishing.

ANDROID APP

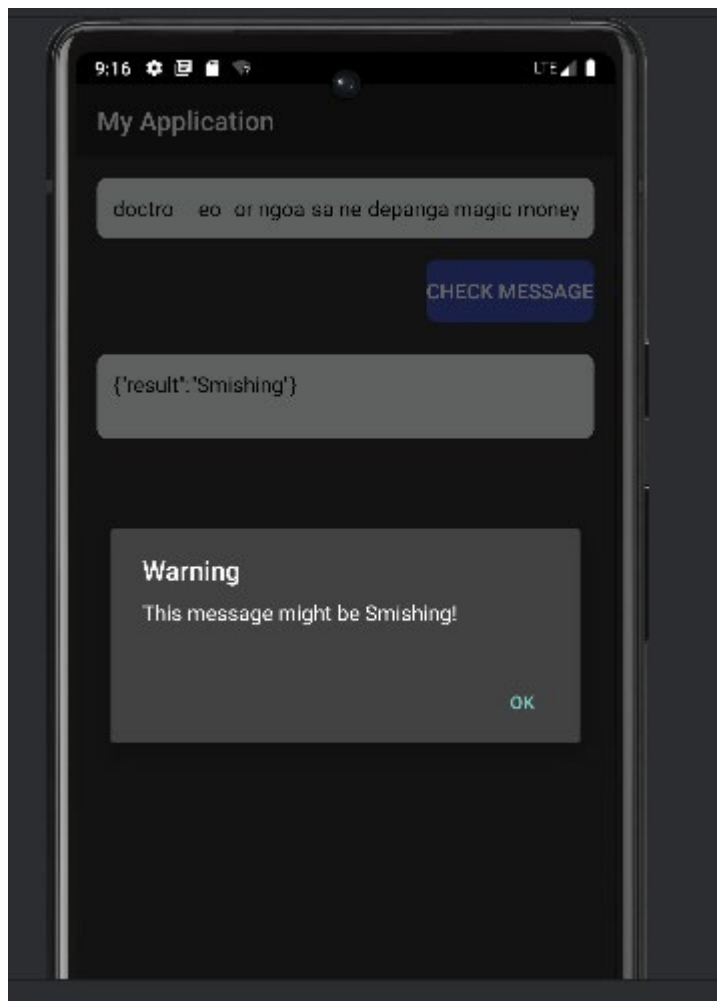
Fig 4.4 Android App UI



Fig 4.5 TELNET CMD SMS SENDING SIMULATION

```
Telnet localhost
Android Console: Authentication required
Android Console: type 'auth <auth_token>' to authenticate
Android Console: you can find your <auth_token> in
'C:\Users\Dell\.emulator_console_auth_token'
OK
auth [REDACTED]
KO: authentication token does not match ~/.emulator_console_auth_token
auth [REDACTED]
Android Console: type 'help' for a list of commands
OK
sms send nine doctor ngosa ndepanga magic money
KO: unknown command, try 'help'
sms send nine doctor ngosa ndepanga magic money
OK
sms send nine doctor ngosa ndepanga magic money
OK
z
```


Fig 4.6 MESSAGE RECEIVED AND RESPONSE OF RESULT



Snippet 6:Sms Receiver code Snippet

```
153
154     private fun setupSmsReceiver() {
155         smsReceiver = SmsReceiver()
156         smsReceiver.setMessageReceivedListener(object : SmsReceiver.MessageReceivedListener {
157             override fun onMessageReceived(message: String) {
158                 runOnUiThread {
159                     messageEditText.setText(message)
160                     // Trigger the warning alert when a message is received
161                     showSmishingAlert()
162                     messageEditText.text.clear()
163                 }
164             }
165         })
166         val intentFilter = IntentFilter(Telephony.Sms.Intents.SMS_RECEIVED_ACTION)
167         registerReceiver(smsReceiver, intentFilter)
168     }
169
```

Snippet 7: HTTP Post Request code Snippet

```
198  private fun sendPostRequest(message: String) {
199      val url = "http://172.20.10.5:5000/detect_smishing"
200
201      val requestBody = RequestBody.create("text/plain".toMediaTypeOrNull(), message)
202
203      val request = Request.Builder()
204          .url(url)
205          .post(requestBody)
206          .build()
207
208      client.newCall(request).enqueue(object : Callback {
209          override fun onResponse(call: Call, response: Response) {
210              val responseBody = response.body?.string() ?: "Empty response"
211              handleSmishingResponse(responseBody)
212              runOnUiThread {
213                  responseTextView.text = responseBody
214              }
215          }
216      })
217  }
```

Fig 4.7 Flask App Running upon received post Request

```
C:\Users\DeLL\AppData\Local\Programs\Python\Python37\python.exe C:\Users\DeLL\AppData\Roaming\JetBrains\PyCharmCE2023.2\scratches\Bemba\smis
* Serving Flask app 'smishing_api'
* Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:5000
* Running on http://172.20.10.5:5000
Press CTRL+C to quit
172.20.10.5 - - [30/Dec/2023 21:15:39] "POST /detect_smishing HTTP/1.1" 200 -
```

CHAPTER 5 RESULTS AND DISCUSSIONS

This section looks at Results Presentation, Analysis of Results, Comparison to Related Work and Implications of Results.

5.1 Results Presentation

Word Cloud

The research processed the dataset and generated a word cloud—a visual representation highlighting the frequency of specific words across both authentic and Smishing messages. This visual aid became instrumental in identifying clusters of words that were markedly more common in one category over the other. Within this exploration, certain words surfaced prominently in Smishing messages, setting them apart from genuine ones. Terms like "Tumeni," "NRC," "Shabalanda," "nashifuma," "nalufma," and "impiya" emerged as recurrent elements within the deceptive messages, showcasing distinct linguistic markers associated with fraudulent or suspicious content of Smishing as show in Fig.

These findings provided invaluable insights into the vocabulary and linguistic patterns characteristic of Smishing attempts. By incorporating these specific terms as features into their model, the research aimed to create a robust framework capable of accurately discerning between authentic messages and potential Smishing threats. The intention was not just to identify individual words but to grasp the broader context and linguistic cues that indicate Smishing intent.

Fig 5.1 Bemba Smishing Word Cloud

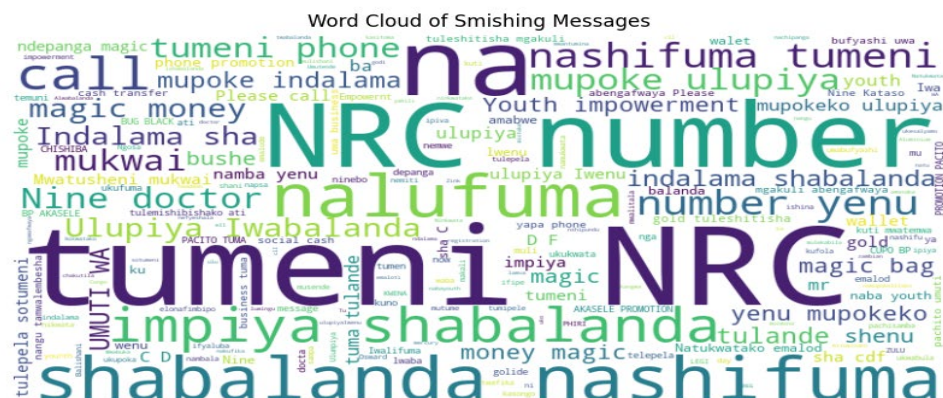


Fig 5.2 English Smishing Word Cloud



Table 5.1 Model Metric Performance:

Metric	Random Forest	Naïve Bayes	Logistic Regression
Matthews correlation coefficient	0.822	0.743	0.822
F1-score (Non-Smishing)	0.90	0.86	0.90
F1-score (Smishing)	0.90	0.84	0.90
Precision (Non-Smishing)	0.83	0.76	0.83
Precision (Smishing)	1.00	1.00	1.00
Recall (Non-Smishing)	1.00	1.00	1.00
Recall (Smishing)	0.82	0.73	0.82

Fig 5.3 Random Forest ROC Curve

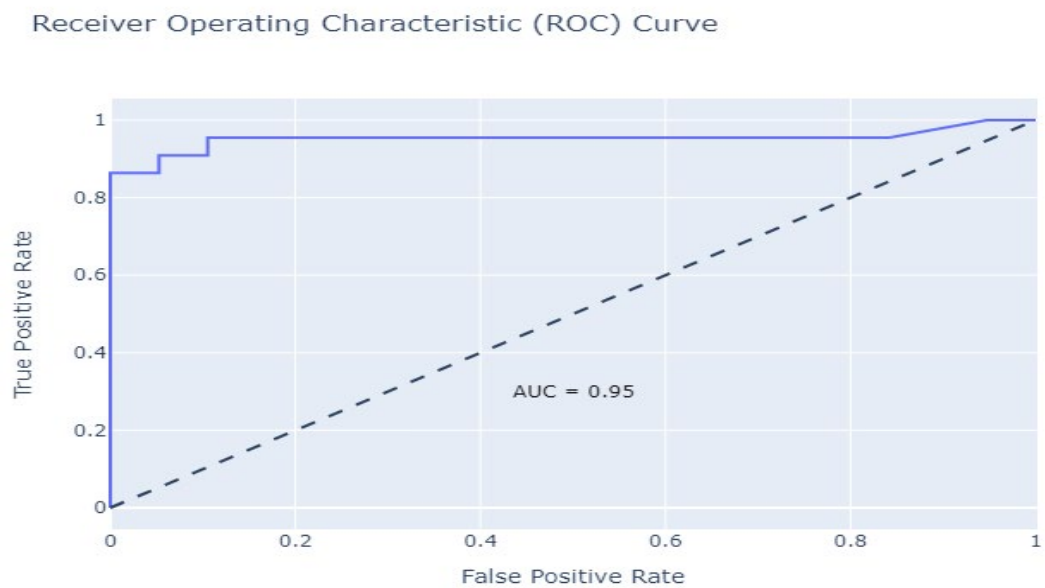


Fig 5.4 Naïve Bayes ROC Curve Fig

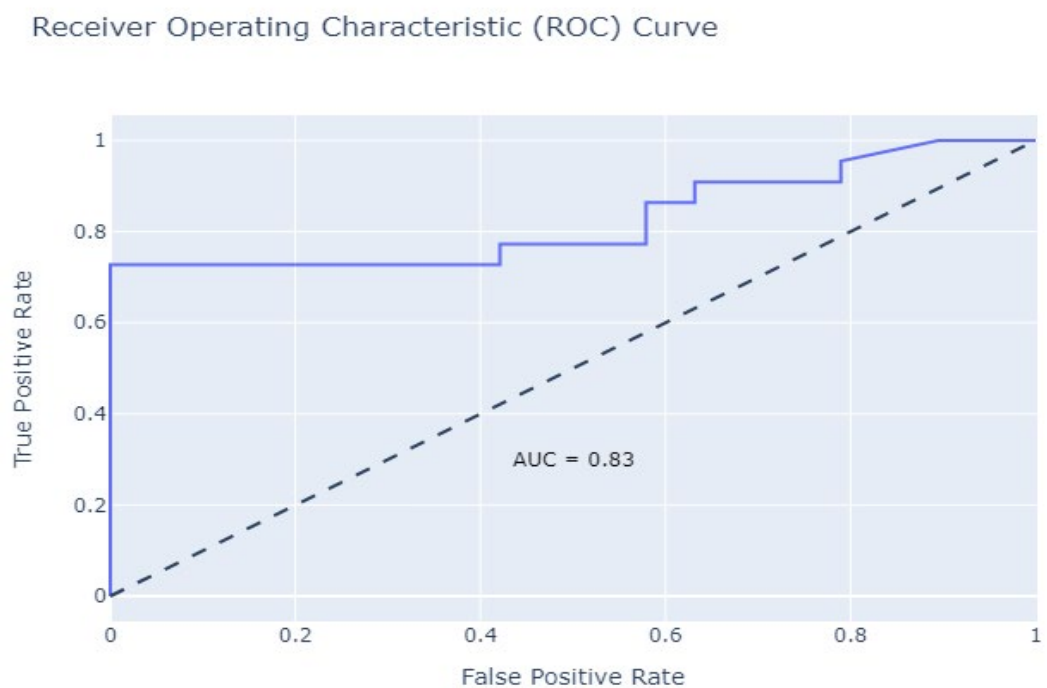
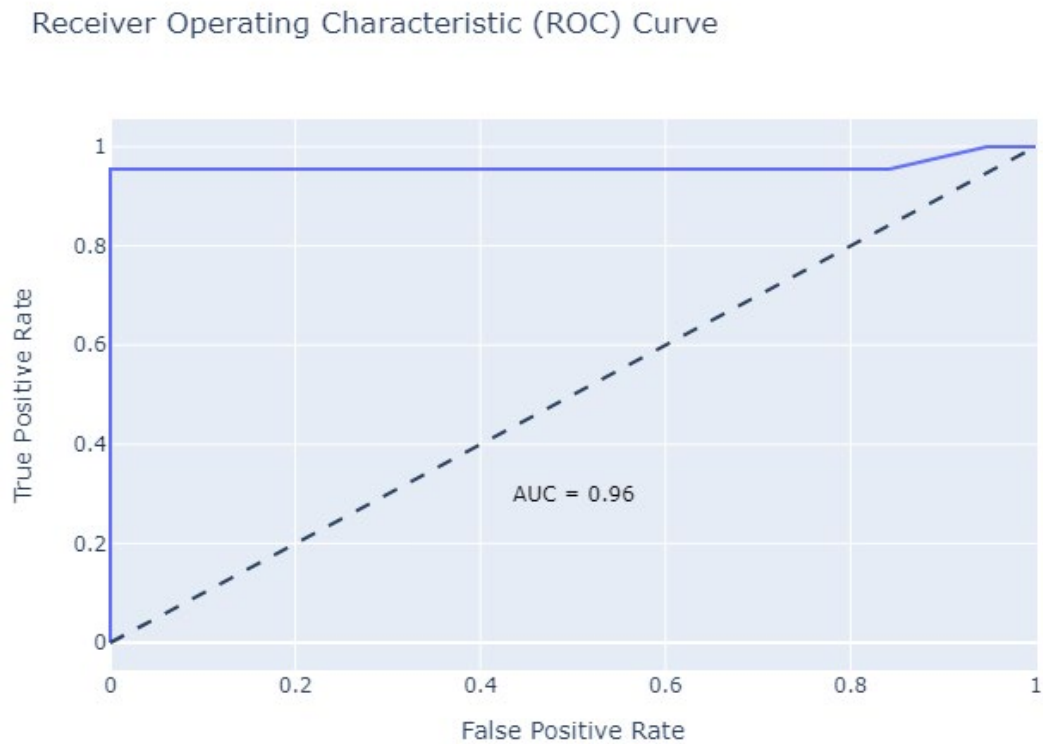


Fig 5.5 Logistic Regression ROC Curve



5.2 Analysis of Results

Model Performance

In the realm of predictive modelling, the evaluation and comparison of various classification algorithms stand as a pivotal moment in understanding their efficacy. Within this subsection, we delve into the performance metrics and results obtained from three distinct classification models: Random Forest, Naïve Bayes, and Logistic Regression. Each model was assessed and scrutinized to determine their effectiveness in distinguishing between smishing (SMS phishing) and non-smishing texts.

Random Forest:

The Random Forest model has cross-validation scores ranging between 0.805 and 0.902, highlighting its consistency in predictive accuracy. Analysing the class distribution shows a near equilibrium between smishing and non-smishing texts, creating a balanced dataset. Moreover, the model identifies key features such as 'label' and 'text' with varying degrees of importance, elucidating crucial insights into the predictive process. The confusion matrix and classification report reveal commendable

performance in discerning between the two classes, demonstrating high precision and recall, resulting in a substantial F1-score of 0.902.

Naïve Bayes:

Comparatively, the Naïve Bayes model presents cross-validation scores ranging from 0.725 to 0.878, showcasing a slightly broader spectrum of predictive accuracy. However, examining the confusion matrix and classification report unveils a slightly lower performance than the Random Forest model with an F1-score of 0.852. Precision and recall metrics for both classes exhibit disparities, indicating areas for potential improvement.

Logistic Regression:

The Logistic Regression model demonstrates cross-validation scores ranging from 0.800 to 0.927, reflecting consistent and high predictive accuracy. Remarkably similar to the Random Forest model, its confusion matrix and classification report exhibit parallel performance, resulting in an identical F1-score of 0.902.

5.3 Comparison of Results to Related Work

Table 5.2 Comparison of Results to Related Work

Attribute/Work	Classifier	Domain	Modelling Approach	F1 Score	AUC Score
Liu et al. (2021)	Logistic Regression	Smishing	Natural Language Processing	93.04	None
Mishra & Soni(2021)	Random Forest	Smishing	Deep Learning	None	0.985
Kipkebut et al. (2019)	Naïve Bayesian	Smishing	Machine Learning	0.961	0.991
(Mambina, Ndibwile, & Michael, 2022)	Random Forest	Smishing	Machine Learning	0.9986	0.9986
Proposed Model	Random Forest	Smishing	Natural Language Processing and Machine Learning	0.902	0.95

5.4 Implication of Results:

The implications drawn from these results can significantly impact decision-making in several ways:

Model Selection:

- **Performance Comparison:**
 - **Random Forest & Logistic Regression:** Both exhibit similar and robust performance across various metrics (Matthews's correlation coefficient, F1-score, precision, recall).

- **Naïve Bayes:** While performing reasonably well, it consistently trails behind the other models across all measured metrics.
- **Implication:** Choosing between Random Forest and Logistic Regression could depend on factors like computational complexity and interpretability.

Detection Accuracy and Reliability:

- **Smishing Detection:**
 - All models demonstrate relatively high accuracy in identifying Non-Smishing messages.
 - Random Forest and Logistic Regression outperform Naïve Bayes in correctly identifying Smishing messages.
- **Implication:** The high performing selected models (Random Forest or Logistic Regression) could effectively aid in identifying Smishing attempts with higher accuracy, contributing to improved security measures.

Further Improvement Opportunities:

- **Optimization and Tuning:**
 - Both Random Forest and Logistic Regression exhibit strong performance, but there might still be room for fine-tuning hyperparameters to enhance accuracy or generalization.

SELECTION: RANDOM FOREST

Random Forest demonstrated robust performance in Smishing detection based on the provided metrics.

Advantages of Random Forest for Smishing Detection:

1. **High Accuracy and Robustness and Model Reliability:**
 - The ensemble nature of Random Forest, aggregating multiple decision trees, often leads to better generalization and reduces overfitting compared to individual trees.
 - Effective in handling high-dimensional data and various types of features, providing flexibility in the types of data it can process.
2. **Interpretability and Insights:**
 - While Random Forest might be less interpretable compared to simpler models like Logistic Regression, efforts in understanding feature importance could yield valuable insights into Smishing characteristics.
3. **Potential for Further Optimization:**

- Despite its robust performance, there may be opportunities to fine-tune the model through hyperparameter optimization or feature engineering for even better accuracy.

CHAPTER 6: SUMMARY AND CONCLUSION

Mobile money transactions have seen an exponential rise globally, offering convenient and accessible financial services to millions. However, this convenience has attracted cyber threats, with smishing emerging as a significant concern. Smishing, a form of SMS phishing, targets users through deceptive text messages to obtain sensitive information or perpetrate fraudulent activities.

The escalating use of mobile money services, combined with the growing sophistication of cybercriminal tactics, underscores the critical need for robust security measures. Developing effective smishing detection models utilizing Machine Learning (ML) and Natural Language Processing (NLP) stands as a crucial defence mechanism to safeguard users and financial transactions.

6.1. The Research Had The Following Findings

Mobile Network Usage:

The dominance of Airtel and MTN in the survey data signifies not just market share but potential risk exposure. This indicates that these networks face specific targeting by smishing attacks due to their larger user bases.

Language in Texts:

Understanding language preferences among users sheds light on the diversity of potential targets for smishing. It also prompts considerations for multilingual detection models to encompass various linguistic patterns exploited in smishing attempts with Bemba been the mostly used local language for smishing attempts

Awareness of Smishing:

The revelation of a majority lacking awareness underscores a critical vulnerability. It emphasizes the urgency for educational initiatives to increase awareness and preparedness against smishing threats and SMishing stands out as the most prevalent form of social engineering attacks amongst mobile phone users closely.

Frequency of Suspicious Messages: Responses varied widely, with some receiving these messages frequently, highlighting a persistent issue.

6.2. Contribution to the Body of Knowledge: Leveraging Nlp and Ml

The research focused on Natural Language Processing (NLP) and Machine Learning (ML) to significantly advance the understanding and detection of smishing, a form of phishing conducted via text messages. The research contributed significantly by:

- **Identifying Linguistic Markers:** Identified specific words characteristic of smishing messages through a word cloud analysis, aiding in understanding linguistic patterns associated with fraudulent texts.
- **Model Performance:** Evaluated multiple ML models (Random Forest, Naïve Bayes, Logistic Regression) for smishing detection, providing insights into their strengths and weaknesses in classification.
- **Model Selection:** Emphasized the robust performance of Random Forest in detecting smishing attempts, offering insights into its advantages over other models.

Linguistic Marker Identification:

The research identified linguistic markers unique to smishing messages. Through a word cloud analysis, specific words and phrases characteristic of Smishing texts were isolated and analysed. This comprehensive linguistic analysis provided a nuanced understanding of the language patterns prevalent in smishing attempts both in Bemba and English. This identification of linguistic markers stands as a crucial step toward developing robust detection mechanisms and enhancing the comprehension of how language is manipulated in deceptive communication such as Bemba

Model Evaluation and Performance:

A comprehensive evaluation of various ML models such as Random Forest, Naïve Bayes, and Logistic Regression was conducted. The aim was to ascertain their efficacy in the detection and classification of smishing attempts. Rigorous testing and analysis were performed to gauge the performance metrics of each model, revealing their respective strengths and weaknesses in handling the complexities of smishing detection leading to Insightful Model Selection for future works similar to the project.

Insightful Model Selection:

Among the array of ML models evaluated, the research emphasized the robust performance of the Random Forest model in accurately identifying smishing attempts. The study provided a detailed analysis outlining the reasons behind its superior performance compared to other models. This emphasis on the Random Forest model was not merely descriptive but offered valuable insights into the underlying mechanisms and advantages that make it particularly adept at detecting smishing, thereby guiding future researchers and practitioners in selecting appropriate models for similar tasks.

6.3 Limitations of the Research Project:

Limited Data:

1. **Restricted Access from Mobile Network Providers:** One significant hurdle encountered in data collection pertains to restricted access to pertinent data from mobile network providers. Due to privacy and regulatory constraints, accessing real-time or historical data related to smishing attempts posed a substantial challenge as mobile network operators often safeguard customer data rigorously, limiting external access to protect user privacy and comply with data protection regulations.
2. **Deletion of Smishing Messages by Users:** Another critical challenge stemmed from user behaviour with the habitual deletion of smishing messages. Individuals receiving suspicious texts, whether due to instinctive caution or lack of awareness about reporting procedures, frequently delete these messages without preserving them. This routine action significantly hampered efforts to gather a comprehensive dataset for analysis and detection model training.

The combination of restricted access from network providers and users' deletion habits significantly impacts the quality and representativeness of the collected data. The available datasets may suffer from incompleteness, bias, or lack of diversity in terms of smishing variations or tactics employed by perpetrators. Consequently, the resultant dataset might not fully capture the breadth and depth of smishing instances, impeding the development of robust detection models.

Limited Awareness among Respondents:

One significant constraint encountered during the research was the prevalence of limited awareness among the surveyed respondents regarding smishing. This lack of familiarity or knowledge about smishing could have potentially influenced the accuracy and reliability of the responses obtained in relation to encounters with such fraudulent activities. As a result, the dataset used for analysis might have been skewed or lacked comprehensiveness due to underreporting or misinterpretation of smishing incidents. This limitation underscores the challenge of studying and comprehensively understanding a phenomenon when a notable portion of the target population remains unaware or uninformed about it.

Model Optimization and Further Room for Improvement:

While the ML models utilized in the research demonstrated commendable performance in detecting smishing attempts, the study acknowledges the potential for further optimization. Despite their effectiveness, there remains a scope for enhancing the models' accuracy and generalization capabilities. Refinements in feature engineering, parameter tuning, or exploring newer algorithms might potentially elevate the models' performance to achieve higher accuracy rates and better generalizability across diverse datasets. The acknowledgment of this limitation highlights the evolving nature of ML models and the perpetual quest for optimization in the realm of predictive analytics.

6.4 Future Works: Advancements and Development

Diversified Data Collection Strategies:

To fortify the robustness and adaptability of the ML models, future endeavors will prioritize the acquisition of more diverse and extensive datasets. This expanded data collection aims to encompass a broader spectrum of smishing instances, including varied linguistic styles, cultural contexts, and evolving techniques employed by cybercriminals. By diversifying the dataset, the models can be trained on a more comprehensive range of scenarios, thereby enhancing their resilience against novel and sophisticated smishing attempts.

Guidance on Reporting Suspicious Messages: The future initiatives aim to empower users by providing guidance on how to handle suspicious messages effectively. The app interface can include a user-friendly mechanism that educates individuals encountering suspicious texts from MTN, Airtel, or similar sources. It would guide them on whether to report, delete, or

ignore the message, emphasizing the importance of reporting such messages to the respective service provider or designated authorities. This guidance ensures users take appropriate action while contributing to collective efforts in combating smishing.

Interactive Reports and Feedback Mechanism: To augment the system's learning and improve its detection capabilities, future iterations can incorporate an interactive reporting feature within the app. Users encountering suspicious messages can directly report them through the app. Additionally, allowing users to provide feedback on false positives or false negatives will be integral. This feedback loop becomes invaluable in refining the system's accuracy over time, ensuring continuous learning and adaptation to evolving smishing techniques.

Improvements in Bemba Language Analysis: Recognizing the significance of linguistic diversity, specific focus needs to be directed towards improving the system's analysis of Bemba language texts. This entails the development or utilization of Bemba-specific word embeddings tailored for semantic representation in the Bemba language context. Moreover, during feature engineering, more attention needs to be given to identifying Bemba stop words, idiomatic expressions, and linguistic patterns unique to Bemba. Integrating these language-specific features will enhance the system's accuracy in detecting smishing attempts in Bemba texts.

Cybersecurity Awareness Campaigns:

An imperative future initiative involves the development and implementation of comprehensive cybersecurity awareness campaigns. These campaigns aim to educate and empower users about the nuances of smishing attacks and how to recognize, report, and protect themselves against such fraudulent activities. By disseminating targeted information through various channels such as workshops, online resources, interactive modules, and social media platforms these campaigns can significantly bolster users' vigilance and resilience against smishing attacks. Additionally, collaboration with cybersecurity experts, government agencies, and educational institutions could amplify the reach and impact of these initiatives.

Model Refinement and Enhancement:

Continued research efforts on the refinement and enhancement of ML models, particularly emphasizing the Random Forest model due to its demonstrated efficacy in smishing detection needs to be done. This involves delving into hyperparameter optimization, fine-tuning model parameters, exploring advanced feature engineering techniques, and potentially integrating

newer algorithms or hybrid models. The goal is to further elevate the accuracy, sensitivity, and specificity of the models, thereby fortifying their ability to effectively discern and combat evolving smishing tactics.

Settings and Customization Options: Recognizing the diversity in user preferences, future iterations of the app can be included as settings for customization. Users can have the flexibility to adjust the sensitivity level for smishing detection or choose their preferred notification methods. This customization empowers users to tailor their app experience to align with their individual needs and preferences.

Security and Privacy Measures: Prioritizing the security and privacy of user data remains paramount. To maintain user trust, stringent security measures need to be implemented within the app. Robust encryption protocols, secure data storage practices, and stringent access controls will be in place to safeguard user information while ensuring the effective functioning of the detection mechanisms.

6.5 Conclusion: The Ongoing Battle against Smishing in Mobile Transactions

The project illuminates the critical importance of cultivating robust smishing detection models within the landscape of mobile transactions. The methodologies and findings showcased throughout this research underline the efficacy of integrating Machine Learning (ML) and Natural Language Processing (NLP) techniques in identifying and mitigating smishing attacks. These advancements serve as pivotal steps toward fortifying the security infrastructure surrounding mobile money transactions.

However, amidst these advancements, a crucial realization emerges the landscape of cyber threats is a dynamic and continuously evolving terrain. The sophistication and adaptability of malicious entities perpetually challenge established defence mechanisms. The very nature of smishing exemplifies this evolution, with perpetrators employing new tactics and variations to bypass existing detection systems. Thus, the research not only signifies progress but also serves as a reminder of the perpetual need for vigilance and adaptation in the realm of cybersecurity.

The synergy between ML and NLP represents a promising frontier in combating smishing. Yet, this battle against cyber threats, particularly in the context of mobile transactions, necessitates unwavering commitment to ongoing research, innovation, and collaboration. Continuous exploration of novel methodologies, the refinement of existing models, and the integration of cutting-edge technologies are imperative to fortify defenses against emerging threats.

Moreover, the symbiotic relationship between technological advancements and cybersecurity initiatives underscores the need for interdisciplinary collaboration. Engineers, data scientists, cybersecurity experts, policymakers, and industry stakeholders must join forces. This collective effort is crucial not only for developing better detection mechanisms but also for fostering a culture of awareness and resilience among users.

In essence, while the integration of ML and NLP stands as a formidable defense against smishing, ongoing dedication, innovation, and collaboration are paramount to outpace and outwit the ever-evolving spectrum of cyber threats within the realm of mobile money transactions. This continuous endeavor serves as the cornerstone for safeguarding the integrity, trust, and security of mobile transaction ecosystems worldwide.

REFERENCES

1. Goel, Diksha & Jain, Ankit. (2018). Smishing-Classifer: A Novel Framework for Detection of Smishing Attack in Mobile Environment. 10.1007/978-981-10-8660-1_38.
 2. Zimba, Aaron & Mbale, Tozgani & Chishimba, Mumbi & Chibuluma, Matthews. (2020). Liberalisation of the International Gateway and Internet Development in Zambia: The Genesis, Opportunities, Challenges, and Future Directions.
 3. Pour, EhsanRahmani & Aliyari, Shahla & Farsi, Zahra & Ghelich, Younes. (2020). Comparing the effects of interactive and noninteractive education using short message service on treatment adherence and blood pressure among patients with hypertension. *Nursing and Midwifery Studies*. 9. 68. 10.4103/nms.nms_82_19.
 4. Adaba, G. B. & Ayoung, D. A., 2017. The Development of a Mobile Money Service: An Exploratory ActorNetwork Study. *Information Technology for Development*, pp. 668-686sing and Midwifery Studies. 9. 68. 10.4103/nms.nms_82_19.
 5. Case of Urban Zambia. *Zambia Social Science Journal*, 7(1), pp. 53-76.
- Kabala, E. & Seshamani, V., 2016. Mobile Technology and Poverty Reduction In Zambia: A SWOT Analysis.
6. D. Goel and A. K. Jain, "Smishing-classifier: A novel framework for detection of Smishing attack in mobile environment," in *Proc. Int. Conf. Gener. Comput. Technol.*, 2017, pp. 502–512.
 7. A. Aleroud, E. Abu-Shanab, A. Al-Aiad, and Y. Alshboul, "An examination of susceptibility to spear phishing cyber attacks in non-English speaking communities," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102614, doi: 10.1016/j.jisa.2020.102614
 8. P. Sethi, V. Bhandari, and B. Kohli, "SMS spam detection and comparison of various machine learning algorithms," in *Proc. Int. Conf. Comput. Commun. Technol. Smart Nation (ICTSN)*, Oct. 2017, pp. 28–31.
 9. S. J. Delany, M. Buckley, and D. Greene, "SMS spam filtering: Methods and data," *Expert Syst. Appl.*, vol. 39, no. 10, pp. 9899–9908, Aug. 2012, doi: 10.1016/j.eswa.2012.02.053

10. Frederick, Laura I. 2014. "Impact of Mobile Money Usage on Microenterprise Evidence from Zambia."
11. Domfeh, H. A. (2018). Moderating the service qualitycustomer loyalty relation through customer satisfaction, gender and banking status: Evidence from mobile money users in university of cape coast, Ghana. *International Journal of Academic Research in Business and Social Sciences*, 8(6), 704-733.
12. . S Mishra, D Soni, (2019) SMS phishing and mitigation approaches. In: Twelfth International Conference on Contemporary Computing (IC3), Noida, India pp. 1–5, doi: 10.1109/IC3.2019.8844920
13. CallHub , "6 reasons why sms is more effective than email marketing - callhub." (2016) URL <https://callhub.io/6-reasons-sms-effective-email-marketing/>, accessed on 2023
14. Delany SJ, Buckley M, Greene D. Sms spam filtering: methods and data. *Expert Syst Appl.* 2012;39(10):9899–9908. doi: 10.1016/j.eswa.2012.02.053.
15. Joo, J.W., Moon, S.Y., Singh, S., Park, J.H.: S-Detector: an enhanced security model for detecting Smishing attack for mobile computing. *Telecomm. Syst.* 66(1), 29–38 (2017)
16. Yadav, K., Kumaraguru, P., Goyal, A., Gupta, A., Naik, V.: Smsassassin: crowdsourcing
17. Foozy, C. F. M., Ahmad, R., & Abdollah, M. F. (2013). Phishingdetection taxonomy for mobile device. *International Journal of Computer Science Issues (IJCSI)*, 10(1), 338–344
18. S. Mishra and D. Soni, "DSmishSMS—A system to detect Smishing SMS," *Neural Comput. Appl.*, vol. 45, pp. 1–18, Jul. 2021.
19. L. Chen, Z. Yan, W. D. Zhang, and R. Kantola, "TruSMS: A trustworthy SMS spam control system based on trust management," *Future Generat.Comput. Syst.*, vol. 49, pp. 77–93, Aug. 2015.

20. B. M. Nturibi, "A mobile money social engineering framework for detecting voice & SMS phishing attacks—A case study of M-Pesa," Ph.D. dissertation, United States Int. Univ. Africa, Nairobi, Kenya, 2018.
21. M. Liu, Y. Zhang, B. Liu, Z. Li, H. Duan, and D. Sun, "Detecting and characterizing SMS spearphishing attacks," in *Proc. Annu. Comput. Secur. Appl. Conf.*, 2021, pp. 930–943
22. A. Kipkebut, M. Thiga, and E. Okumu, "Machine learning SMS spam detection model," in *Proc. Kabarak Univ. Int. Conf. Comput. Inf. Syst.*, C. M. Maghanga and M. Thiga, Eds., Nakuru, Kenya: Kabarak Univ., Oct. 2019, pp. 63–70
23. A. K. Jain and B. B. Gupta, "Feature based approach for detection of Smishing messages in the mobile environment," *J. Inf. Technol. Res.*, vol. 12, no. 2, pp. 17–35, Apr. 2019.
24. The Social Engineering Framework. <https://www.social-engineer.org/framework/attackvectors/smishing/>. Accessed 02 July 2023
25. Mercy W. Buku and Rafe Mazer. *Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System*. World bank publications, 2017. <https://documents1.worldbank.org/curated/en/249151504766545101/pdf/119208-BRI-PUBLICBrief-Fraud-in-Mobile-Financial-ServicesApril-2017.pdf>
26. Hakeem J. Pallangyo. *Cyber Security Challenges, its Emerging Trends on Latest Information and Communication Technology and Cyber Crime in Mobile Money Transaction Services*, *Tanzania Journal of Engineering and Technology*, 41(2):189-204, 2022. <http://dx.doi.org/10.52339/tjet.v41i2.792>.
27. A. K. Jain and B. B. Gupta, "Rule-based framework for detection of Smishing messages in mobile environment," *Proc. Comput. Sci.*, vol. 125, pp. 617–623, Mar. 2018.
28. Castle, Pervaiz Fahad, Cassebeer WeldGalen, Roesner Franziska and Richard J. Anderson. *Let's Talk Money: Evaluating the Security Challenges of Mobile Money in the Developing World*. In *Proceedings of the 7th Annual Symposium on Computing*

for Development (ACM DEV '16, 18 – 20 November 2016, Nairobi, Kenya, 1-10, 2016.
<https://doi.org/10.1145/3001913.3001919>

29. I. S. Mambina, J. D. Ndibwile and K. F. Michael, "Classifying Swahili Smishing Attacks for Mobile Money Users: A Machine-Learning Approach," in *IEEE Access*, vol. 10, pp. 83061-83074, 2022, doi: 10.1109/ACCESS.2022.3196464.
30. Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018. <https://translatorswithoutborders.org/language-data-for-zambia/>
31. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. In *Future Internet* (Vol. 11, Issue 4). <https://doi.org/10.3390/FI11040089>
32. Language data for Zambia. (n.d.). *Translators without Borders*. Retrieved November 5, 2023, from Upadhyay, P., & Jahanyan, S. (2016). Analysing user perspective on the factors affecting use intention of mobile-based transfer payment. *Internet Research*, 26 (1), 38–56. <https://doi.org/10.1108/IntR-05-2014-0143>