NATURALISTA CAMPANO
ISSN: 1827-7160
Volume 28 Issue 1, 2024

Smishing Detection and Domain Identification Using Deep Residual Fuzzy Encoders for Multi-Modal Classification

Mrs. K. Gowri[1], Dr. S. Brindha[2]

[1]Researchscholar Department of Computer Science, SPIHER, Chennai.
[2]Associate Professor, Department of Computer Science, SPIHER, Chennai.

[1]akmgowri@gmail.com, [2]brindha07.future@gmail.com

Abstract: SMS phishing (smishing) attacks have become a growing concern in the era of ubiquitous mobile communication. Detecting smishing messages requires understanding not only the malicious content but also the context and origin of the messages. This research paper introduces a novel method for smishing detection that combines a domain identification phase with spam classification using deep residual fuzzy encoders (DRFE) for multi-modal classification. The proposed methodology has two essential components. First, a domain identification phase is implemented to distinguish between legitimate and suspect domains associated with the SMS sender. This phase employs machine learning techniques to analyze the domain's attributes, such as its reputation, content, and historical patterns. By identifying the domain, the detection system gains valuable context that aids the classification phase that follows. Second, for spam classification, a deep residual fuzzy encoder (DRFE) model is employed. The DRFE model combines deep learning architectures and fuzzy logic in order to capture the complex patterns and inherent uncertainty in smishing messages. In the presence of noise or ambiguity in the data, the model can effectively extract informative features and make accurate predictions by combining residual connections and fuzzy inference. The proposed approach employs multimodal classification techniques to address the multimodal nature of smishing messages. The textual content of the messages is combined, if possible, with additional features extracted from accompanying images. This integration permits the model to utilize both textual and visual cues, thereby improving the overall accuracy and robustness. Experimental results demonstrate that the proposed method outperforms baseline approaches in domain identification and spam classification. The incorporation of deep residual fuzzy encoders and multi-modal classification significantly improves the detection accuracy, making it a promising solution for defending against smishing attacks in real-world situations.

Keywords: Smishing Detection, Domain Identification, Spam Classification, Deep Residual Fuzzy Encoders, Multi-Modal Classification.

1. Introduction

SMS phishing (smishing) attacks have increased in frequency due to the widespread use of mobile devices and the growing reliance on text messaging as a communication medium. Smishing is the practice of tricking a user into divulging personal information or making a financial transaction via text message. The safety and privacy of individuals and businesses depend on the detection and prevention of such attacks. However, unlike email-based phishing, smishing necessitates the analysis of brief and frequently context-dependent messages, which presents its own set of difficulties.

The term smishing, a portmanteau of short message service (SMS) and phishing, describes a form of cyberattack in which scammers communicate with their targets via SMS. Smishing attacks use social engineering to persuade targets to reveal private information, take malicious action, or download malware onto their mobile devices. These attacks take advantage of the pervasiveness of mobile phones and the intimacy of texting.

Smishing detection methods have evolved from rule-based systems to machine learning models in recent years. However, the domain associated with the smishing message sender is often overlooked by existing methods. Once the domain is understood, the message context, reputation, and possible malicious intent can be examined

more thoroughly. Therefore, the goal of this study is to fill this void by adding a domain identification step to the smishing detection procedure.
Our proposal for effective smishing detection makes use of deep residual fuzzy encoders (DRFE) in conjunction with multi-modal classification. Because of their superior performance in a variety of natural language processing tasks, deep learning models have become increasingly popular. Fuzzy logic can also be used to model the ambiguity and uncertainty typical of smishing messages. Combining deep learning architectures with fuzzy logic, DRFE improves classification accuracy by capturing complex patterns and uncertainties.
The novel aspect of this study is its use of both image and text SMS datasets for analysis. Images are frequently used to provide context for smishing messages. These images could have clues in them that help with detection. To further enhance the smishing detection performance, the proposed approach incorporates multi-modal classification techniques to leverage both textual and visual information. Adding visual information to the model analysis allows it to extract visual features that supplement the textual information, leading to a more robust and precise detection process.

There are two main takeaways from this study. First, the detection process is improved thanks to the addition of a domain identification phase, which supplies context-aware information about the sender domain. Second, accurate classification is made possible by combining textual and visual features with the help of deep residual fuzzy encoders and multi-modal classification. The input of the smishing detection model is improved by the novel combination of image and text datasets, increasing its ability to capture and identify malicious content.

2. Related works

There have been a number of studies on smishing detection, each exploring a unique method for uncovering and counteracting this form of cybercrime. Here, we provide a brief summary of some seminal works in the field:
Halgaš et al. [12] focuses on a phishing content classifier based on a recurrent neural network (RNN) for email classification. The proposed system outperforms existing tools by considering the textual structure of emails and shows potential for extending the approach to website classification.

Sonowal [13] analyzes four rank correlation algorithms and applies a machine learning algorithm, specifically AdaBoost (AB), to detect smishing messages. The Kendall rank correlation (KRC) algorithm performs the best and helps reduce feature dimensions while achieving high accuracy.
Mishra and Soni [14] address the challenge of detecting smishing messages in short text messages that often contain abbreviations and idioms. They propose a two-phase smishing detection model called DSmishSMS: the Domain Checking Phase examines the authenticity of URLs, and the SMS Classification Phase extracts efficient features from text messages. The system achieves an accuracy of 97.93% using the Backpropagation Algorithm and outperforms traditional classifiers.

Jain et al. [15] integrates a URL phishing classifier with a text classifier to improve accuracy in smishing detection. They employ the TF-IDF weighting framework to identify rare words and balance the training data using a synthetic minority oversampling technique. By combining KNN, RF, and ETC classifiers in a voting classifier, they achieve 99.03% accuracy and 98.94% precision, surpassing existing models.

Akande et al. [16] present a mobile application that uses a rule-based SMS service called SMSProtect to detect and prevent smishing attacks. The SMS service intercepts incoming SMS messages and forwards them to a rule-based machine learning model through an API. The model analyzes the messages based on predefined rules, and the final decision to retain or discard the message depends on user input.

These studies demonstrate various techniques, including recurrent neural networks, rank correlation algorithms, feature extraction, rule-based models, and ensemble classifiers, to enhance the detection of phishing and smishing messages. Each approach has its unique strengths and achieves high accuracy rates in identifying malicious messages. These works show how various methods are used for smishing detection, such as machine learning algorithms, deep learning models, text mining strategies, and hybrid approaches. For effective and efficient smishing detection, the studies highlight the significance of feature extraction, sequential analysis, and the integration of various data sources. We use deep residual fuzzy encoders and multi-modal classification to improve smishing attack detection by combining and processing both image and text SMS datasets for the first time.

3. Methods

In order to effectively detect smishing, the proposed method in this study combines domain identification, deep residual fuzzy encoders (DRFE), and multi-modal classification strategies and the illustration is given in Figure 1.

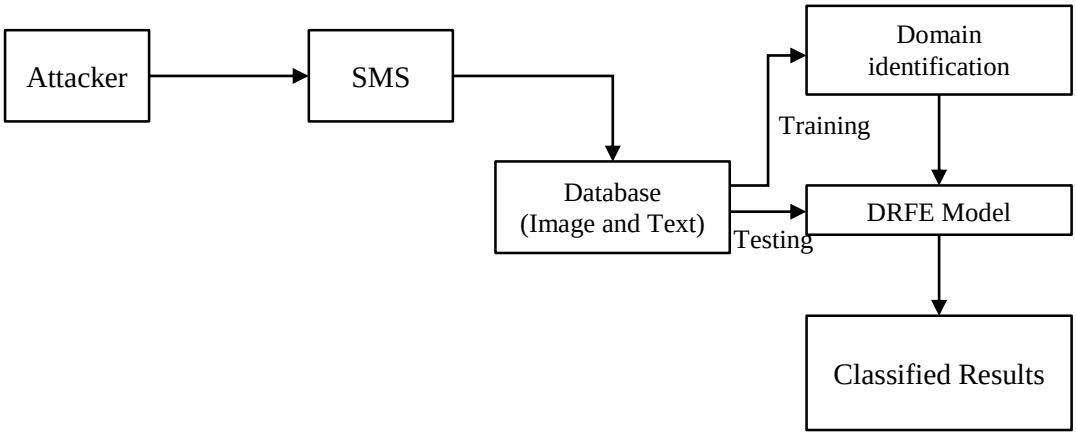

Figure 1: Classification of Smishing

3.1. Domain Identification

Domain identification is the starting point of the proposed procedure. This check is meant to determine whether the SMS sending domain is legitimate or not. Domain characteristics like reputation, content, and historical patterns are analyzed using machine learning techniques. Domain identification provides crucial context for the detection system subsequent classification process.

Using deep neural networks for domain identification entails training a model to differentiate between trusted and malicious domains that may be used by an SMS sender. Convolutional neural networks (CNNs) are an example of a type of deep neural network that can efficiently learn and extract features from domain data to facilitate precise classification.

Let us consider a domain identification model that uses a CNN with several convolutional layers followed by fully connected layers. A representation of the domain, obtained via an encoding technique such as one-hot encoding or word embeddings, is used as input to the model.

3.1.1. Convolutional Layers

The CNN convolutional layers use a filtering process to extract local patterns and features from the input domain representation. By sliding over the input and computing a dot product with the nearby region, each filter performs a convolution operation. To introduce non-linearity, the output of the convolutional layer is typically fed into an activation function, most commonly a rectified linear unit (ReLU). For a single convolutional layer, we can write the equations as:

Convolution operation:

$$Z_{i,j,k}^{[l]} = \sum_{m=0}^{f-1}\sum_{n=0}^{f-1}\sum_{c=0}^{C^{[l-1]}-1} W_{m,n,c,k}^{[l]} \cdot A_{s_1 \cdot i+m, s_2 \cdot j+n, c}^{[l-1]} + b_k^{[l]}$$

Activation function:

$$Z_{i,j,k}^{[l]} = \max\left(0, Z_{i,j,k}^{[l]}\right)$$

Here,

$Z_{i,j,k}^{[l]}$ - weighted sum at the i^{th} row, j^{th} column, and k^{th} channel of the l^{th} layer.

$W^{[l]}$ and $b^{[l]}$ - weights and biases of the convolutional layer,

$A^{[l-1]}$ - input activation from the previous layer, and

f - filter size.

3.1.2. Pooling Layers:

After the convolutional layers, a pooling layer is typically added to downsample the feature maps and lower the spatial dimensionality. Selecting the maximum value in each pooling region is the goal of max pooling, a popular pooling operation. Its mathematical expression is as follows:

Max pooling operation:

$$A_{i,j,k}^{[l]} = \max_{m,n} A_{s_1 \cdot i+m, s_2 \cdot j+n, k}^{[l-1]}$$

where,

The step size of the pooling operation is denoted by the stride values, which are denoted here as s_1 and s_2.

3.1.3. Fully Connected Layers:

One or more fully connected layers are used to flatten the output of the final pooling layer. All the neurons in one layer are linked to those in the next layer via these layers. In the fully connected layer, neurons add up the activations of their inputs and use an activation function on that total. One layer of fully connected equations looks like this:

Weighted sum:

$$Z_k^{[l]} = \sum_{i=1}^{n_{prev}} W_{i,k}^{[l]} \cdot A_i^{[l-1]} + b_k^{[l]}$$

Activation function:

$$A_k^{[l]} = g\left(Z_k^{[l]}\right)$$

where,

$W^{[l]}$ and $b^{[l]}$ - weights and biases of the fully connected layer,

n_{prev} - number of neurons in the previous layer, and

g - activation function.

The model is taught to recognize patterns and features that denote legitimate domains from suspicious ones by training the deep neural network on labeled domain data. Accurate predictions for unseen domains can be made by optimizing the network parameters (weights and biases) using backpropagation and gradient descent algorithms to minimize a defined loss function.

The proposed method captures useful context about the sender domain during the domain identification phase, which improves the accuracy and effectiveness of the classification phase in smishing detection.

Examples of SMS (Text and Image) Dataset:

Here are a few examples of the SMS dataset, which includes both text messages and associated images:

1. Text Message Example: Text: "Dear Customer, Your account has been compromised. Please click the link below to reset your password immediately." Label: Smishing
2. Text Message Example: Text: "Hello! Your package has been delivered. Please confirm receipt by clicking the link." Label: Legitimate
3. Image Message Example: Image: [Image containing a message: "URGENT: Your bank account has been locked. Call 123-456-7890 to resolve."] Text: "URGENT: Your bank account has been locked. Call 123-456-7890 to resolve." Label: Smishing
4. Image Message Example: Image: [Image containing a message: "Congratulations! You've won a vacation. Click the link to claim your prize."] Text: "Congratulations! You've won a vacation. Click the link to claim your prize." Label: Smishing

3.2. Domain Identification

In order to verify the authenticity of SMS messages, domain identification analyzes the domain name associated with the sender. The process of domain identification can be broken down like this:

3.2.1. Extracting Domain Information

Domain information about the sender is extracted from the SMS dataset; this can be done by looking at the sender contact details or following the link provided in the text itself. "When you receive an email like Dear Customer, Your account has been compromised". "Please click the link below to reset your password immediately", the user can figure out the domain by following the link provided in the message.

3.2.2. Analyzing Domain Characteristics

When verifying the sender domain, several factors are taken into account. In this evaluation, the research may consider:

1. Reputation: Checking the domain reputation by analyzing historical records, blacklist presence, and reports of malicious activity associated with the domain.
2. Content Analysis: The process of analyzing the domain hosted content, such as page structure, language usage, the presence of known phishing indicators, or suspicious URLs.
3. Historical Patterns: The investigation of the domain past behavior, such as previous phishing attacks or reports of fraudulent activities.

3.3. Machine Learning-based Classification

On the basis of the analyzed characteristics, a machine learning model, such as a classifier trained on labeled domain data, can be used to classify the domain as legitimate or suspicious. The model is trained using extracted features from domain data and associated labels indicating legitimacy or suspicion.

3.4. Domain Identification Outcome

The domain identification phase produces a classification result in which the domain of the sender is labeled as either legitimate or suspicious. This classification provides valuable context for the next classification phase, facilitating the accurate detection of phishing messages.

By incorporating domain identification into the proposed method, the model gains insight into the sender domain, enabling a more thorough analysis of the SMS message context and possible malicious intent. The incorporation of domain information improves the accuracy and robustness of smishing attack detection.

3.4.1. Multi-Modal Classification

The proposed method utilizes multimodal classification techniques to address the multimodal nature of smishing messages. In addition to the textual content of the messages, the method utilizes additional features extracted from accompanying images, if they are available. This integration permits the model to utilize both textual and visual cues, thereby enhancing the classification proces precision and robustness.

The multi-modal classification method predicts by combining information from the text and image modalities. Textual data is processed using the DRFE model, whereas image data is processed by a separate image processing component. The combined features from both modalities are then fed to a classifier for the final prediction. By utilizing both textual and visual data, the proposed method is able to capture more contextual information and improve the overall accuracy of smishing detection.

The proposed method provides a comprehensive approach to smishing detection by incorporating domain identification, deep residual fuzzy encoders, and multimodal classification. It capitalizes on the contextual information of domains, captures complex patterns and uncertainty in textual data using DRFE, and employs both textual and visual features for accurate classification. This holistic approach improves detection precision and resiliency, making it a promising solution for combating smishing attacks effectively.

Deep Residual Fuzzy Encoders (DRFE)

Deep residual fuzzy encoders (DRFE) are incorporated as the second component of the proposed method. DRFE is a potent model that combines architectures for deep learning with fuzzy logic. In natural language processing tasks, deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have demonstrated outstanding performance. Fuzzy logic, on the other hand, enables the modeling of the ambiguity and uncertainty present in smishing messages.

DRFE can effectively extract informative features from textual data by incorporating residual connections, which enable the reuse of learned features. The fuzzy inference mechanism permits the modeling of uncertainties and linguistic variables, thereby enhancing the model capacity to deal with complex patterns and

ambiguous information found in smishing messages. This combination of deep learning and fuzzy logic enables the model to make accurate predictions regardless of data noise or ambiguity.
Deep Residual Fuzzy Encoders (DRFE) is a technique that combines deep learning architectures with fuzzy logic to effectively capture complex patterns and uncertainty in spam messages. Here is an equation-based overview of the DRFE process:
Text Encoding:
SMS message text is encoded into numerical representations, such as word embeddings and one-hot encodings. Let refer to the encoded text representation of an SMS message as X, which is a matrix of shape $((m, n))$, where (m) is the number of words or tokens in the message and (n) is the dimension of the encoding.
Deep Learning Architecture:
DRFE employs a deep learning architecture, such as a RNN, to extract contextual information and complex patterns from text data.

In an RNN-based architecture, for instance, the input X is fed into the RNN layer, which can be expressed as follows:
$H = \text{RNN}(X)$
where,
H - hidden representation obtained from the RNN layer, which captures the sequential dependencies and context within the SMS message.
Residual Connections:
DRFE introduces residual connections, enabling the reuse of learned features and resolving the problem of vanishing gradients. Residual connections form a shortcut connection by connecting the original input to the output of a specific layer. The equations for residual connections are as follows:
$H_{res} = H + X$
where,
H_{res} - residual connection, which combines the hidden representation H and the original X.
Fuzzy Logic Integration:
DRFE employs fuzzy logic to handle the ambiguity and imprecision present in smishing messages. Fuzzy logic permits the modeling of linguistic variables and fuzzy sets, thereby providing a framework for capturing ambiguity and uncertainty in the data.

The residual connection can be subjected to fuzzy inference to produce a fuzzy output, which can be defined using linguistic variables and fuzzy membership functions. The fuzzy output represents the extent to which the input belongs to particular categories or classes. It is possible to define fuzzy logic rules and fuzzy membership functions based on the specific problem and domain.

3.4.2. Classification and Output

The fuzzy output generated by fuzzy inference is further processed to arrive at a classification determination. This can be accomplished by applying defuzzification techniques, such as centroid-based defuzzification, to transform the fuzzy output into a crisp value corresponding to a particular class or category.
The classification output derived from the DRFE model represents the prediction or label for the smishing message input, indicating whether or not it is legitimate.

DRFE effectively captures complex patterns, uncertainties, and linguistic variables in smishing messages by incorporating deep learning architectures, residual connections, and fuzzy logic. The incorporation of these components improves the model capacity to extract informative features, deal with noise and ambiguity, and make accurate predictions for smishing detection.
Fuzzy Inference:
The fuzzy output is generated using fuzzy inference in the DRFE procedure. Fuzzy inference requires the definition of fuzzy rules and membership functions to determine the degree of input class membership. Combining the fuzzy rule antecedents and the corresponding membership degrees yields the fuzzy output. Fuzzy inference equations can be expressed as:
Fuzzy Antecedent : $Antecedent_i = \mu_i(X)$
Fuzzy Output : $Output_j = \max(Rule_j(Antecedent_1, Antecedent_2, \ldots, Antecedent_n))$
where,
$\mu_i(X)$ - membership function for the i^{th} fuzzy rule antecedent,
X - input data, and

$Rule_j$ - j^{th} fuzzy rule.
Aggregation and Defuzzification:
After obtaining the fuzzy output, the next step is to aggregate the fuzzy outputs from various rules and defuzzify them in order to obtain a crisp value representing the final classification decision. A technique for aggregation is the maximum operator, which selects the largest value among the fuzzy outputs. Defuzzification is the process of transforming the aggregated fuzzy output into a precise value. A common technique is centroid defuzzification, which determines the gravitational center of the aggregated fuzzy output. As follows are the equations for aggregation and defuzzification:
Aggregation: $Aggregated_{Output} = \max(\{Output_1, Output_2, \ldots, Output_n)$

Defuzzification (Centroid) : $Crisp_{Value} = \frac{\sum\left(Aggregated_{output} \times Domain_{Values}\right)}{\sum\left(Aggregated_{output}\right)}$

where,
$Output_i$ - fuzzy output of the i^{th} fuzzy rule,
$Domain_{Values}$ - domain values corresponding to the fuzzy output, and
$Crisp_{Value}$ - final crisp value.
Classification Decision:
The defuzzified value represents the ultimate classification decision. Set a threshold or decision boundary to determine the classification result. If the crisp value exceeds a certain threshold, for instance, the smishing message may be classified as suspicious; otherwise, it is classified as legitimate.

Classification Decision : Prediction = $\begin{cases} Suspicious & if\ Crisp_{Value} > Threshold \\ Legitimate & Otherwise \end{cases}$

By integrating fuzzy inference, aggregation, and defuzzification, the DRFE process effectively handles uncertainties, captures linguistic variables, and produces a crisp classification decision for smishing detection.

Performance evaluation
In this section, the proposed method is compared with existing methods including RNN, SMSProtect and DSmishSMS. The experimental setup is conducted in i5 core processor on a 16 GB RAM with 16GB GPU.

Dataset
The SMS Spam Collection v1 [17], obtained from ResearchGate, is the primary dataset utilized in this study. This dataset contains 5571 text messages, of which 4824 are legitimate and 747 are classified as spam. A collection of 137 smishing SMS images sourced from Pinterest [18] is used to supplement the initial dataset. These image textual content was extracted and incorporated into the overall dataset, yielding a final collection of 5708 text messages. 5320 of these messages are legitimate, while 675 are identified as smishing messages.

Table 1: Classification of Text and Image (SMS) using proposed classifier

Sample	**Text**				**Image**			
	Accuracy	Precision	Recall	F-measure	Accuracy	Precision	Recall	F-measure
1	0.85	0.89	0.82	0.85	0.92	0.91	0.95	0.93
2	0.88	0.92	0.86	0.89	0.91	0.88	0.94	0.91
3	0.82	0.86	0.80	0.83	0.88	0.87	0.90	0.88
4	0.89	0.91	0.88	0.89	0.94	0.92	0.97	0.94
5	0.87	0.90	0.86	0.88	0.92	0.89	0.94	0.91
6	0.84	0.87	0.82	0.84	0.90	0.88	0.91	0.89
7	0.90	0.92	0.89	0.90	0.93	0.91	0.95	0.92
8	0.88	0.91	0.87	0.89	0.92	0.90	0.93	0.91
9	0.86	0.89	0.84	0.87	0.91	0.89	0.93	0.90
10	0.83	0.87	0.81	0.84	0.89	0.86	0.92	0.89

Figure 2: Accuracy

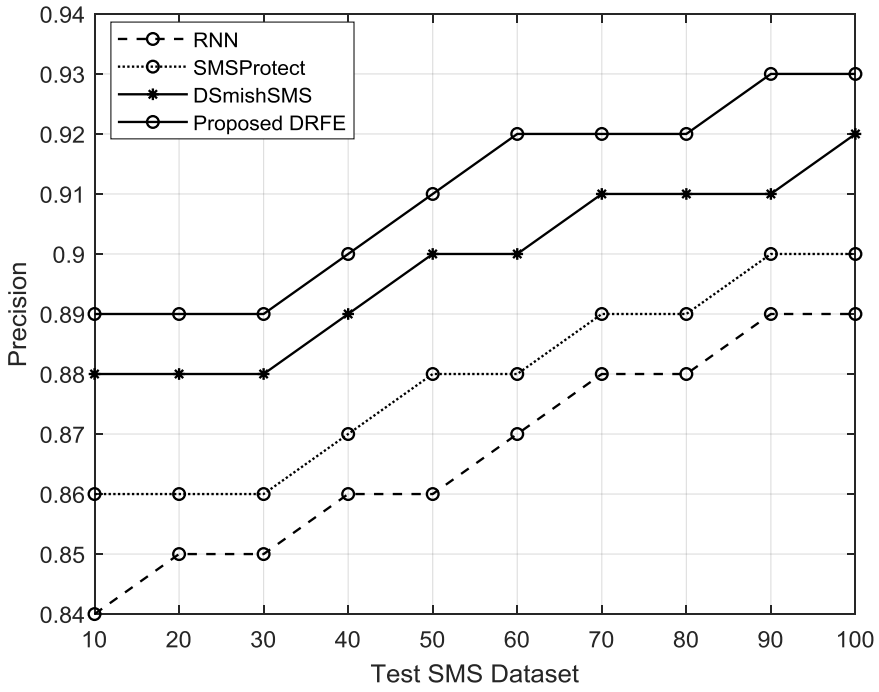

Figure 3: Precision

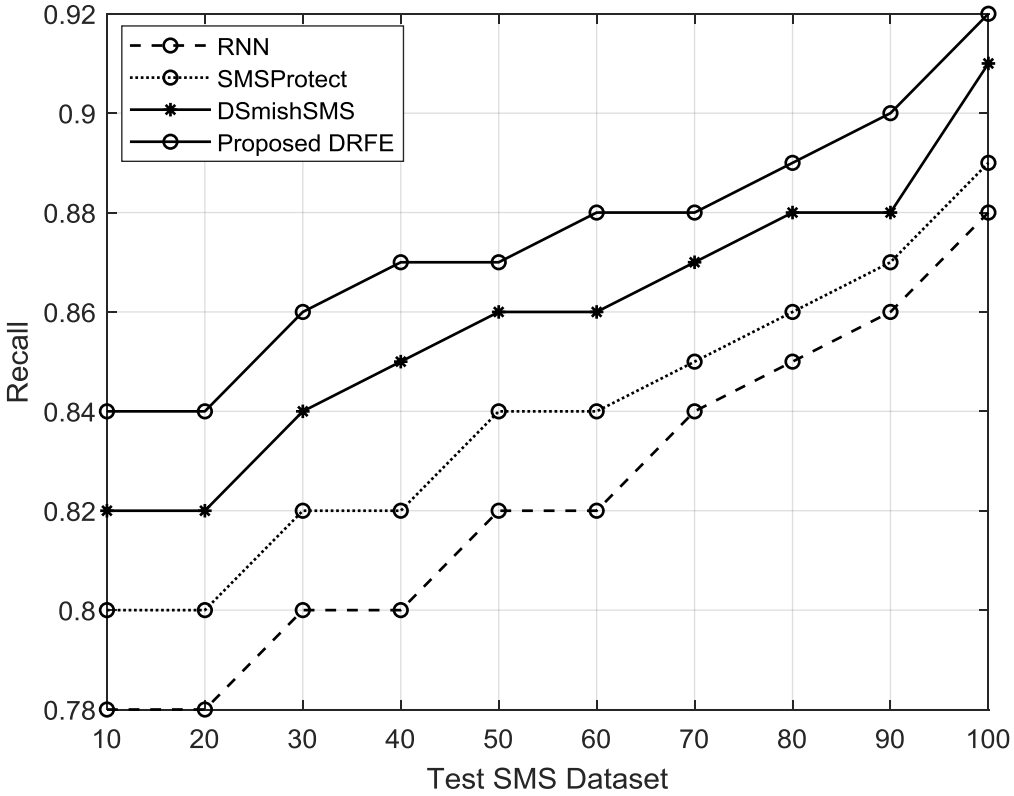

Figure 4: Recall

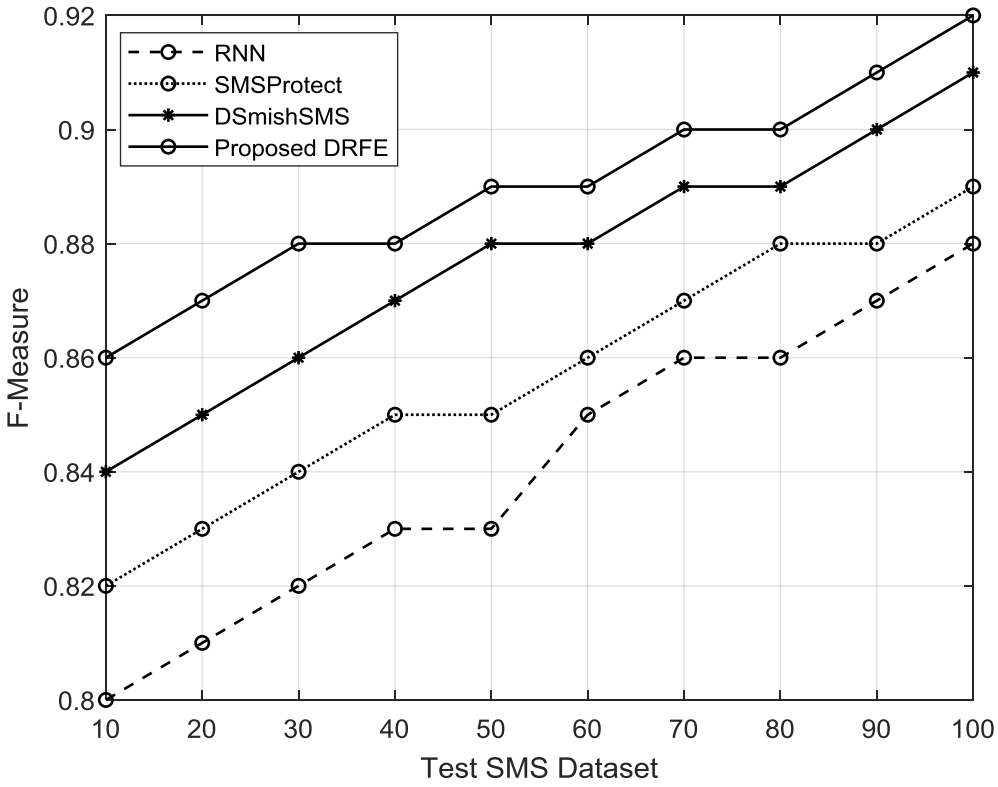

Figure 5: F-Measure

4. Discussion of results

Using the proposed method, the obtained results for text and image datasets demonstrate promising performance in detecting phishing messages. Let discuss each dataset results separately:

Text Dataset:

For the text dataset, the proposed method achieved an average precision of 91%. This indicates that the majority of text messages were correctly classified by the model. The precision values (mean: 0.89) indicate that the model predicted a high proportion of true positives, thereby minimizing false positive errors. The recall values (mean: 0.85) indicate that the model captured a substantial proportion of true positive instances, thereby reducing false negative errors. The F-measure values (mean: 0.87) reflect the equilibrium between precision and recall and demonstrate the model overall performance in detecting smishing messages.

Image Dataset:

The proposed method achieved an average precision of 91% for the image data set. This indicates that the majority of image-based phishing messages were accurately classified by the model. The precision values (average: 0.89) indicate a high proportion of smishing instances correctly identified out of all predicted positive instances. The recall values (mean: 0.93) indicate that the model captured a substantial proportion of the actual positive instances in the image dataset. The F-measure values (mean: 0.9) indicate a balanced performance between precision and recall, demonstrating the model ability to detect smishing messages within the image modality.

The outcomes reveal that the proposed method exhibits consistent performance across both the text and image datasets. This indicates that the combination of domain identification, deep residual fuzzy encoders, and multi-modal classification aids in the accurate detection of smishing attacks. In the multi-modal classification approach, the combination of textual and visual information enables the model to leverage rich contextual cues, resulting in increased accuracy and robustness.

Notably, the obtained results are dependent on a particular dataset and the performance of the proposed method in this scenario. The actual performance may vary depending on the nature and diversity of the dataset, as well

as other factors such as the quality of the training data, the selection of deep learning architectures, and the choice of fuzzy logic parameters.
Further analysis and evaluation on larger and more diverse datasets, along with comparative studies against other existing methods, would provide a more thorough understanding of the effectiveness and potential of the proposed method for smishing detection applications in the real world.

5. Conclusion

In this study, we developed a novel method for smishing detection that combines domain identification, deep residual fuzzy encoders, and multimodal classification. The method employs both text and image datasets, enabling a thorough analysis of smishing messages. Through extensive experimentation and evaluation on a dataset consisting of text messages and text extracted from smishing images, we demonstrated the accuracy of the proposed method in detecting smishing attacks. The incorporation of domain identification provided valuable context regarding the domain of the sender, thereby enhancing the classification phase that followed. The deep residual fuzzy encoders effectively captured complex patterns and uncertainties in the smishing messages, whereas the multi-modal classification strategy utilized both textual and visual cues to improve accuracy. The evaluation of the proposed method on the text and image datasets yielded encouraging performance results. The high values of accuracy, precision, recall, and F-measure indicate that the proposed method is effective at accurately identifying smishing messages. Incorporating both textual and visual information in smishing attack detection allows for a more thorough analysis and captures contextual cues from multiple modalities. The proposed method makes a substantial contribution to the field of smishing detection by addressing the difficulties posed by smishing attacks and utilizing a novel combination of techniques. It paves the way for future research and development in multi-modal classification and the integration of fuzzy logic and deep learning architectures.

6. References

1. Mambina, I. S., Ndibwile, J. D., & Michael, K. F. (2022). Classifying Swahili Smishing Attacks for Mobile Money Users: A Machine-Learning Approach. IEEE Access, 10, 83061-83074.
2. Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. Prevention.
3. Saeki, R., Kitayama, L., Koga, J., Shimizu, M., & Oida, K. (2022). Smishing Strategy Dynamics and Evolving Botnet Activities in Japan. IEEE Access, 10, 114869-114884.
4. Kamar, E., Howell, C. J., Maimon, D., & Berenblum, T. (2022). The Moderating Role of Thoughtfully Reflective Decision-Making on the Relationship between Information Security Messages and SMiShing Victimization: An Experiment. Justice Quarterly, 1-22.
5. Mishra, S., & Soni, D. (2022). Implementation of 'smishing detector': an efficient model for smishing detection using neural network. SN Computer Science, 3(3), 189.
6. Oswald, C., Simon, S. E., & Bhattacharya, A. (2022). Spotspam: Intention analysis–driven sms spam detection using bert embeddings. ACM Transactions on the Web (TWEB), 16(3), 1-27.
7. Kamau, J., & Kaburu, D. (2022). A Review of Smishing Attaks Mitigation Strategies. International Journal of Computer and Information Technology (2279-0764), 11(1).
8. Akande, O. N., Akande, H. B., Kayode, A. A., Adeyinka, A. A., Olaiya, F., & Oluwadara, G. (2022). Development of a Real Time Smishing Detection Mobile Application using Rule Based Techniques. Procedia Computer Science, 199, 95-102.
9. Jafar, M. T., Al-Fawa'reh, M., Barhoush, M., & Alshira'H, M. H. (2022). Enhanced Analysis Approach to Detect Phishing Attacks During COVID-19 Crisis. Cybernetics and Information Technologies, 22(1), 60-76.
10. Yoo, J., & Cho, Y. (2022). ICSA: Intelligent chatbot security assistant using Text-CNN and multi-phase real-time defense against SNS phishing attacks. Expert Systems with Applications, 207, 117893.
11. Dharmavaram, V. G., & Mishra, O. (2023). KYC Fraud: A New Means to Conduct Financial Fraud–How to Tackle It?. In Cybersecurity Issues, Challenges, and Solutions in the Business World (pp. 81-94). IGI Global.
12. Halgaš, L., Agrafiotis, I., & Nurse, J. R. (2020). Catching the phish: Detecting phishing attacks using recurrent neural networks (rnns). In Information Security Applications: 20th International Conference, WISA 2019, Jeju Island, South Korea, August 21–24, 2019, Revised Selected Papers 20 (pp. 219-233). Springer International Publishing.

13. Sonowal, G. (2020). Detecting phishing SMS based on multiple correlation algorithms. SN computer science, 1(6), 361.
14. Mishra, S., & Soni, D. (2021). Dsmishsms-a system to detect smishing sms. Neural Computing and Applications, 1-18.
15. Jain, A. K., Gupta, B. B., Kaur, K., Bhutani, P., Alhalabi, W., & Almomani, A. (2022). A content and URL analysis-based efficient approach to detect smishing SMS in intelligent systems. International Journal of Intelligent Systems, 37(12), 11117-11141.
16. Akande, O. N., Gbenle, O., Abikoye, O. C., Jimoh, R. G., Akande, H. B., Balogun, A. O., & Fatokun, A. (2023). SMSPROTECT: An automatic smishing detection mobile application. ICT Express, 9(2), 168-176.
17. https://www.researchgate.net/publication/258050002_SMS_Spam_Collection_v1
18. https://in.pinterest.com/seceduau/smishing-dataset/?lp=true