SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Hybrid Model For Multi-Feature SMS And URL Safety Classification Using Machine Learning

M.P. Sudha[1*], Dr.M. Ramesh Kumar[2]

[1*]Research Scholar, PG and Research Department of Computer Science, Government Arts College (Autonomous), Nandanam, Chennai, Tamil Nadu, India. E-mail: mpsudhacsdgvc@gmail.com, https://orcid.org/0009-0006-1290-5378

[2]Associate Professor and Head, PG and Research Department of Computer Science, Government Arts College (Autonomous), Nandanam, Chennai, Tamil Nadu, India. E-mail: proframeshkumar@gmail.com, https://orcid.org/0000-0001-5345-2762

*Corresponding author: Email: mpsudhacsdgvc@gmail.com

Abstract

SMS and phishing a serious cybersecurity thread in mobile user. This article recommends a hybrid machine learning model framework that combines both Support Vector Machines (SVM) for optimal hyperplane-based classification and Random Forest (RF) ensemble learning to improve Security across textual features that are extracted from TF-IDF and URL-based features generated from lexical and structural patterns. In addition, sentiment analysis provides important understanding into user wish and behaviour of text message. An integrating machine learning system for multi-task classification inclusion of SMS spam detection, malicious URL identification, and sentiment analysis is presented in this Hybrid model. A Hybrid model to increase accuracy and reliability communications that are believed to come from reliable sources, such as banking sectors, trusting delivery services, and government Authorities incorporates predictions from both classifiers associations Random Forest (RF) and Support Vector Machine (SVM). The SVMRF model outperforms compare the individual SVM obtained 82% accuracy, 80% F1-score and RF achieved 77.82% accuracy, 77% F1-score when tested on a standard messaging dataset, SVMRF model providing higher accuracy for real-time mobile security thread. The model suggested that real-world mobile communication services is established by classification accuracy, overall accuracy is obtained 86%, it indicates that reliable performs of multifeatured SMS and Malicious URL SVMRF classification model

Keywords: SVMRF .SMS. TF-IDE, Cybersecurity, Malicious URL, Machine learning.

1. Introduction

Text message is a reliable communication till now and worldwide using these services, but its ease of attackers spread vulnerable to sophisticated attacks. Text messages are a direct and high-open-rate route that attackers utilize for thread in the form of Malicious URL, also known as smishing, which results SMS security is critical in different Sectors like data breaches, financial fraud, and identity theft. It is a prime target because of its easy availability on mobile devices, which affect security trust and significant losses if misused. The increased mobile messaging usage of has led to a boost in spam messages and dangerous URLs. Additionally, sentiment analysis has become essential role in understanding user thought and communication behaviour because SMS lacks built-in encryption technique, messages might be hacked during transmission. When Attackers send fake messaging and phishing URL from banks or other services like businesses and customers are exposed to hazards. Safeguarding it keeps mobile user confident and avoids losses from violations. The Figure 1 shows a hybrid multi-task classification SVMRF model framework for harmful URL identification, and SMS spam detection include sentiment analysis using safe and malicious URL prediction. It demonstrates how input data convert into feature fusion and used hybrid modelling SVMRF classification outputs for secure mobile information. Attackers use different kind of format for user distraction like masking real domains after a "." symbol and add some extra domain like fakebank@malicious.site.com) or URL encoding insert malicious URLs in SMS that to be similar trustworthy websites.

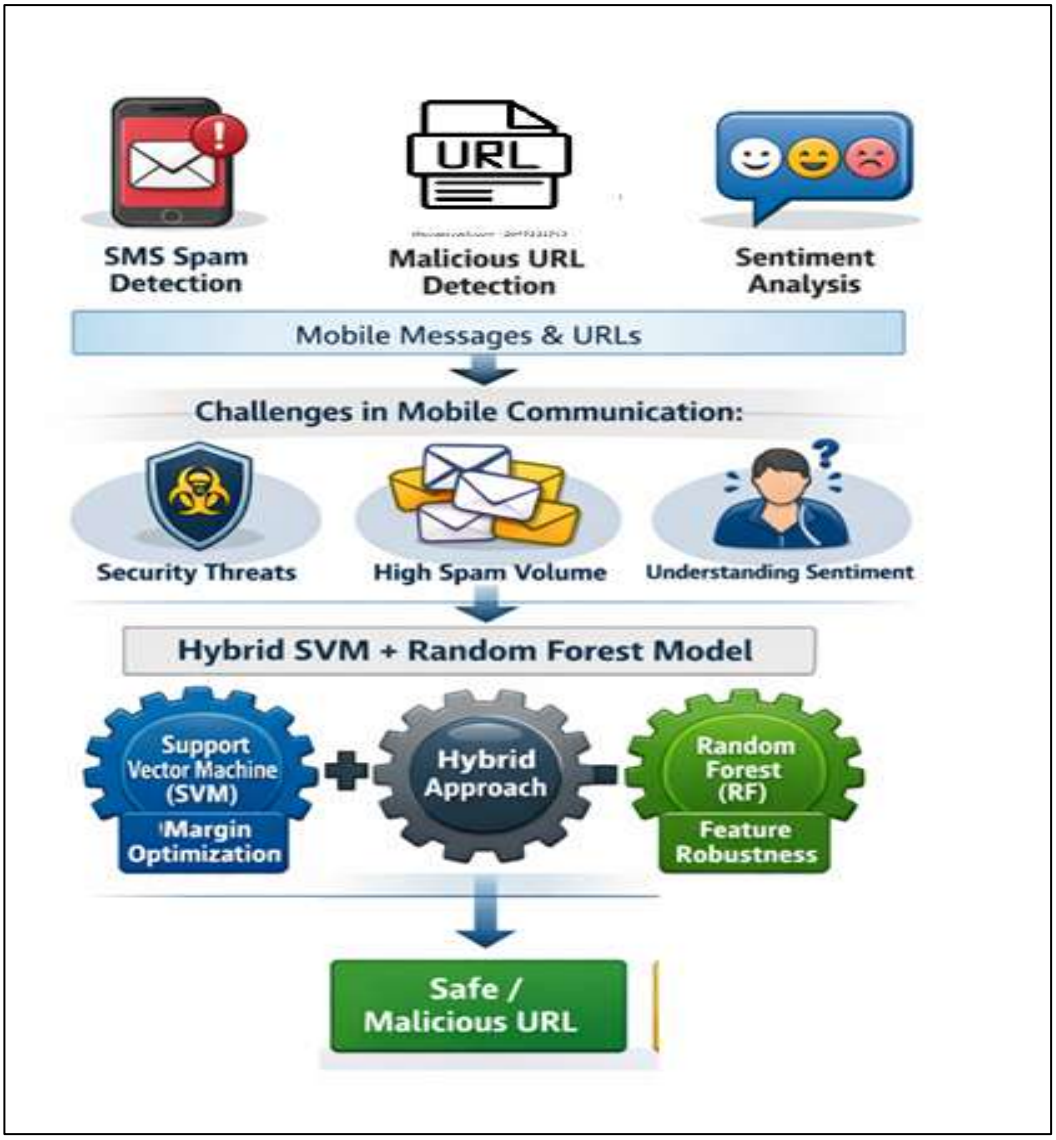

Figure1: Overview for Multi-Task Classification

When user click the link present in SMS data, they are redirected on phishing pages that take advantage of their faith in well-known businesses strategies now- a- days and stealing passwords through phony login forms or Captchas. Scammers use emotions tone like "Your account will be suspended! “Or greed “Claim your prize now! “To get people click on links quickly because emotions word avoids analyse of hacker’s behaviours. In order to authorities and personalize messages with context from data breaches build urgency and weaken barriers by traditional spam detection systems,URL-based threats are frequently ignored concentrate on message content. This article Section2 Literature review, section3 methodology of SMS security, explain how scammer manipulation and misleading URLs to trick users, section 4 result and discussion for safety measures.

2. Literature Review

A recent research in 2026 that looked at the result of feature representation using TF-IDF and n-grams found that classifiers like SVM and Random Forest yield acceptable accuracy when combined with suitable preprocessing and feature selection methods used in machine learning classifier [1].Similar this way, according to a spam sms and phishing detection is most important in cybersecurity thread focused study from 2025 [2].Ensemble and hybrid learning methodologies to increase their performance because detecting fraudulent SMS and phishing a 2025 study an ensemble model suggested that combination of SVM and Random Forest, showing better classification accuracy and fewer false positives than individual models [3]. This demonstrates Hybrid architectures have also tired interest in the field of deep learning classifier, how well hybrid techniques

handle noisy and complex text data using NLP. A fuzzy logic and BiLSTM-based explainable model was presented in a 2025 study that maintained good accuracy in SMS spam classification while improving interpretability [4].Similar to this, hybrid deep learning models that combine CNN and BERT have been suggested for smishing detection; these models get better results by extracting contextual and character-level features [5].Additionally, recent studies highlight cybersecurity-focused smishing detection systems, where hybrid deep learning models improve detection performance against changing threats.

Combining many deep learning approaches greatly enhances the detection of SMS-based phishing assaults, according to a 2024 study [6]. Hybrid frameworks that combine statistical characteristics and anomaly detection have demonstrated encouraging outcomes for malicious URL detection. The significance of URL-based feature engineering was demonstrated by a 2025 study that found great accuracy (over 96%) utilizing a combination of feature extraction, anomaly filtering, and machine learning classifiers [7]. Multi-task learning, which combines sentiment analysis and spam identification, is another significant area of study. In recent research suggested hybrid frameworks models outperformed compare to single-task models [8]. The benefit of common feature representations across machine learning and lexical tasks is emphasized by these methods. Furthermore, more popular research becomes multilingual and cross-lingual spam detection. A 2026 study multilingual SMS data and unbalanced datasets that used GAN-based data augmentation showed better results when managing Large language models (LLMs) for spam detection. Traditional classifiers like SVM and RF is still inexpensive using TF-IDF in conjunction, even proving that recent technique in deep learning models. This shows improved balanced performance and efficiency can be achieved higher accuracy through hybrid approaches that combine tradition and advancement techniques.

3. Proposed Methodology

The suggested multitask hybrid machine learning classification system for sentiment analysis, harmful URLs, and Spam text. To increase overall accuracy and reliability, the model using data preprocessing, feature extraction makes fusion dataset finally hybrid classification model.

A. Preprocessing

To improve accuracy, removing noise and make a quality of dataset, data preprocessing methods is an essential step to removing unwanted data such as Stopwords, punctuation, and special characters are eliminated from the given text data. including, all text is conversion, Stemming is used to reduce words size after tokenization, which divides the text into meaningful individual parts. For URLs, normalization extracting meaningful tokens.and removing prefixes such as “http” and “www. This technique ensures that both textual and URL data are in a suitable format for feature extraction.

B. Feature Extraction

Three kinds of Technique applied in Fusion dataset:

1) Text Features

- msg_length
- word_count
- digit_count
- url_count

2) URL Features

- URL length
- Number of special characters
- Domain-based features
- number of dots
- has_https

3) Sentiment Features

- Polarity positive and subjective scores

C. Feature Fusion

To enhance classification performance used in single unified feature vector is created by combining the features that were retrieved from the text, malicious URL, and sentiment scores. The fusion may learn combine various feature types because multi-task learning within a single framework is made possible in large part by feature fusion.

A fusion feature vector is created by: Fusion**=F [text + URL +Sentiment]**

D. Hybrid Classification Model

Integrated model suggested that two machine learning methods are Support Vector Machine (SVM) and Random Forest (RF) supported to Hybrid classification. SVM is ability to optimal decision limit efficiency and managing high dimensional data in text classification tasks performs well with a vast feature. Conversely, Random Forest prediction accuracy an ensemble learning technique that builds multiple decision trees and aggregates their results. By averaging overfitting noise a. A hybrid strategy is observed to utilize on their advantages of both paradigms. A voting class technique is used to integrate predictions from Random Forest with SVM. Compared to individual classification, Hybrid fusion increases classification accuracy and provide reliable communication.

$F_{Hybrid} = [F_{SVM} + F_{RF}]$

E. Multi-Task Classification

Three categorization tasks are carried out concurrently by the system.:

- Spam Detection: Finds out whether a message is spam or ham
- URL Classification: Finds out whether a URL is safe or malicious.
- Sentiment Analysis: Determines sentiment as Positive, Negative, or Neutral

The system increases efficiency and decreases computational redundancy by combining various activities into a single model. Fusion Strategy

- Voting by majority or weighted
- SVM and RF outputs are combined.

Architecture Flow

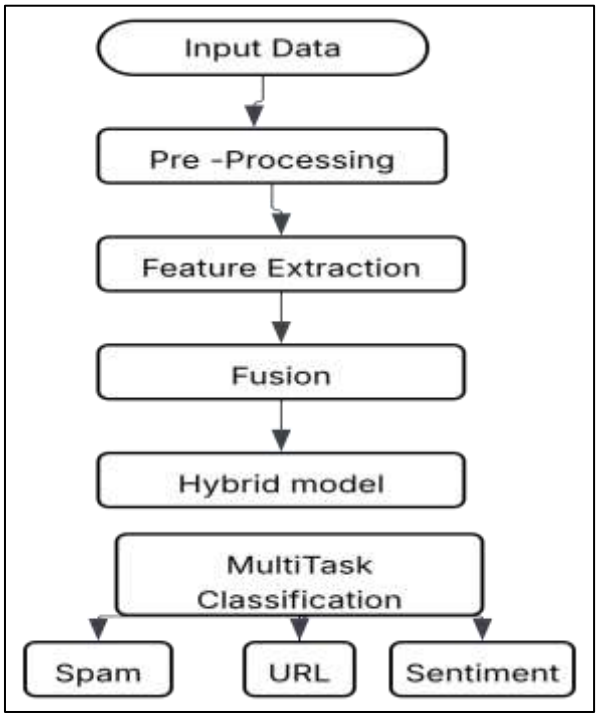

Figure 2: Architecture of Multitask classification

A. Performance Evaluation

The recommended hybrid framework uses a feature fusion technique to combine SMS textual data , URL-based attributes and sentiment score. these fused feature data sets were utilized to assess the performance SUMRF classification: Support Vector Machine (SVM), Naïve Bayes (NB). Table 1 shows individual and comparative performance of models trained on SMS-only features, URL-only features, and sentiment scores.

Table I: Performance analysis of Classification Models

Model	Features	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
SVM	SMS Only	80	81	80	81
SVM	URL Sentiment	75	74	76	75
SVM	Fusion	82	79	81	80
RF	SMS Only	75	77	79	78
RF	URL Sentiment	70	69	71	70
RF	Fusion	77.82	76	78	77
Hybrid (SVM+RF)	Feature Fusion	86	80	81	82

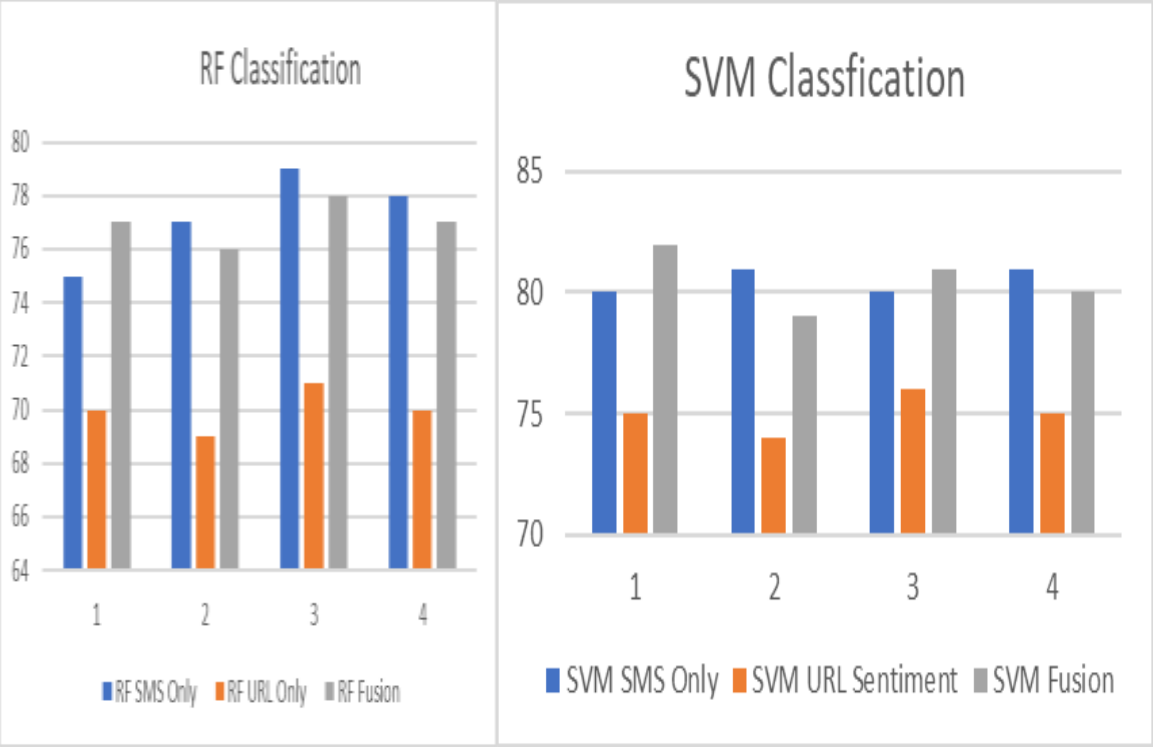

Figure 3: Performance Comparison of SVM and RF

Figure 3 shows in The Random Forest (RF) and Support Vector machine classifier's performance analyse using separate feature settings—SMS-only, URL-only analyses and fusion Features in SMS dataset. Here the RF model consistently obtains the highest accuracy 75% in text classification, whereas URL-only features perform the worst accuracy 70% Although the fusion approach's peak accuracy is marginally lower than that of SMS-only models. SVM results obtained 82% produces in fusion feature and text classification, URL separate Features is lower accuracy obtained, Figure 4 indicating merging both feature types and Hybrid indication.

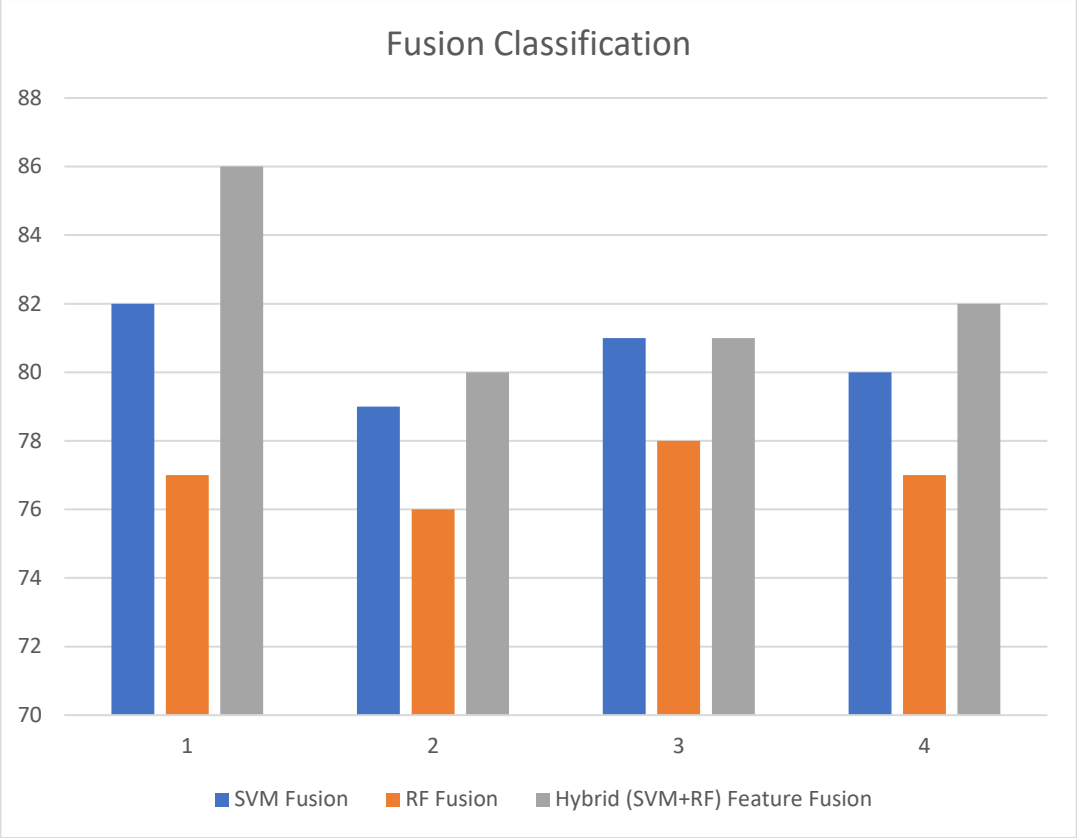

Figure 4: Multitask Fusion classification Analysis

B. Analysis of Results

The findings figure 4 Multitask classification analysis that the hybrid model performs better than individual classifiers in every evaluation metric. SVMRF model increase in accuracy shows how well SVM and Random Forest work together for multi-task classification. While Random Forest successfully captures complex feature interactions, the SVM model processing at high-dimensional textual data. The hybrid model powers the complementary strengths of both models by combining them.

C. Task-wise Performance

1) SMS Spam Detection

The SVM model elegant accuracy for spam and authentic messages. Classification performance result was greatly enhanced by the technique of TF-IDF characteristics.

2) URL Classification

URL-based characteristics achieved highest accuracy in SVM model but Malicious links were easier to spot thanks to the addition of including length and unusual characters identified in RF classification. The hybrid model decreased false positives, when compared to single classifiers.

3) Sentiment Analysis

The scammer used variety of text expressions cues to a reasonable level of accuracy in sentiment classification. Nevertheless, overall system control was enhanced by incorporating sentiment score.

D. Impact of Feature Fusion

Multiple parts of data captured by the SMS dataset to finding a key factor in improving model performance was feature fusion. Attribute of the data were captured by the dataset through the combination of text, URL, and sentiment. As a result, all tasks produced better classification and generalization results. The model does, however, have several drawbacks. Real-time performance may be impacted by the hybrid approach's increased

processing complexity. Furthermore, sophisticated deep learning methods can increase the accuracy of sentiment analysis.

E. Comparative Insight

The suggested system provides a complete framework for sentiment analysis, URL classification, and spam detection in contrast to traditional methods that concentrate on a single task. Because of this, it is more suited for mobile communication systems in the real world where there are numerous risks and analytical needs.

4. Conclusion

A SVMRF machine learning model framework for multi-task categorization of sentiment analysis, malicious URL detection, and SMS spam detection. The proposed Model to take advantage of Random Forest (RF) ensemble learning approaches and Support Vector Machine (SVM) margin-based approaches. The accuracy efficiently measures many aspects of mobile communication features by integrating feature-level fusion of textual, URL-based, and sentiment elements. With an overall accuracy SVMRF model is achieved 80%, classification result show that the SVMRF model performs better than separate classifiers. Emotion categorization in addition strength of the model demonstrates a high capacity to identify harmful URLs and detect spam messages. Single processing the unified model take multi-task framework to improves computing efficiency and minimizes redundancy. The proposed model offers a reliable and scalable solution for safe consideration of all things and intelligent mobile message analysis, it All making appropriate for real time uses in mobile communication and cybersecurity systems. Future work will focus on improving the fusion-based SMS, URL, sentiment categorization framework using cutting-edge deep learning models like LSTM, CNN, and Transformer architectures.

References

1. Soysaldı Şahin, M., Şahin, D. Ö., & Salah, A. F. (2026). Revisiting SMS spam detection: The impact of feature representation on classical machine learning models. Electronics, 15(4), 894. https://doi.org/10.3390/electronics15040894
2. Johari, M. F., Chiew, K. L., Hosen, A. R., et al. (2025). Key insights into recommended SMS spam detection datasets. Scientific Reports, 15, 8162. https://doi.org/10.1038/s41598-025-92223-1
3. Xu, H., Qadir, A., & Sadiq, S. (2025). Malicious SMS detection using ensemble learning and SMOTE to improve mobile cybersecurity. Computers & Security, 154, 104443. https://doi.org/10.1016/j.cose.2025.104443
4. Jasim, A. K., Al-Ibraheemi, F. A., & Alkaabi, H. A. (2025). Explainable AI for SMS spam filtering: A novel hybrid architecture combining fuzzy logic and bidirectional LSTM networks. Franklin Open, 14, 100466.
5. Tanbhir, G., Shahriyar, M. F., Shahed, K., Chy, A. M. R., & Al Adnan, M. (2024). Hybrid machine learning model for detecting Bangla smishing text using BERT and character-level CNN. In 2024 13th International Conference on Electrical and Computer Engineering (ICECE) (pp. 57–60). IEEE. https://doi.org/10.1109/ICECE64312.2024.10860882
6. Mahmud, T., Prince, M. A. H., Ali, M. H., Hossain, M. S., & Andersson, K. (2024). Enhancing cybersecurity: Hybrid deep learning approaches to smishing attack detection. Systems, 12(11), 490. https://doi.org/10.3390/systems12110490
7. Khaled, B., & Zeraoulia, R. (2025). A hybrid deep learning and anomaly detection framework for real-time malicious URL classification (arXiv:2512.03462). arXiv.
8. Şahin, M. S., Şahin, D. Ö., & Salah, A. F. (2026). Revisiting SMS spam detection: The impact of feature representation on classical machine learning models. Electronics, 15(4), 894. https://doi.org/10.3390/electronics15040894
9. Filali, A., Shorfuzzaman, M., Abdellaoui Alaoui, E., et al. (2026). Cross-lingual SMS spam detection using GAN-based augmentation for imbalanced datasets. Scientific Reports, 16, 7128. https://doi.org/10.1038/s41598-026-37769-4
10. Ahmadi, M., et al. (2025). Leveraging large language models for cybersecurity: Enhancing SMS spam detection with robust and context-aware text classification (arXiv:2502.14856). arXiv.