SMART SHIELD: A REAL-TIME, LANGUAGE-AWARE SYSTEM FOR SMS SPAM DETECTION

Kuber Abrol [1], Khushi Mittal [1], Karan Singh [1], Hitesh [1], Dr. Monika Garg [1]

[1] Department of Computer Science & Engineering, Echelon Institute of Technology, Faridabad, India

Received 21 June 2024
Accepted 23 July 2024
Published 31 August 2024

DOI
10.29121/granthaalayah.v12.i8.2024.6101

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

The proliferation of SMS spam presents a significant challenge in modern mobile communication, resulting in user dissatisfaction, reduced trust in messaging services, and heightened security vulnerabilities such as phishing attacks and data breaches. Traditional spam detection methods often fall short in handling the dynamic and evolving nature of spam content, especially in real-time environments where speed and accuracy are critical. This study introduces a comprehensive, real-time SMS spam filtering system designed to deliver high performance with minimal latency.

The proposed system leverages machine learning techniques, enhanced by advanced natural language processing (NLP) methodologies, to identify and filter spam messages with precision. The research focuses on key elements essential to real-time classification: robust data preprocessing pipelines, effective feature engineering strategies, and the selection of lightweight yet powerful machine learning algorithms suitable for deployment on mobile and cloud-based infrastructures.

To address the challenge of detecting increasingly sophisticated spam content, the system incorporates NLP-based techniques such as tokenization, lemmatization, and context-aware embeddings, enabling it to capture nuanced linguistic patterns and deceptive language often used by spammers. Extensive experiments demonstrate the system's capability to maintain high accuracy and low false-positive rates while operating within strict time constraints.

Furthermore, the system is designed with adaptability and scalability in mind, supporting integration with various messaging platforms and compatibility with multiple languages. This ensures its applicability in diverse communication environments, from enterprise-level applications to individual user devices. The research underscores the potential of combining real-time processing with intelligent language understanding to offer a proactive and resilient defense against SMS spam.

1. INTRODUCTION

Given its current content, SMS (Short Message Service) remains a widely used communication method in today's world of continual connectivity. Despite the rise of instant messaging platforms and social media, SMS retains its relevance due to its simplicity, universality across mobile devices, and reliability in areas with limited internet access. It continues to be the communication method of choice for a range of services including banking, healthcare, government alerts, and two-factor authentication [1]. SMS is not only a preferred choice for personal communication but also serves as a vital tool for businesses to engage with customers, send alerts,

How to cite this article (APA): Abrol, K., Mittal, K., Singh, K., Hitesh, and Garg, M. (2024). Smart Shield: A Real-Time, Language-Aware System for SMS Spam Detection. *International Journal of Research - GRANTHAALAYAH, 12*(8), 174–185. doi: 10.29121/granthaalayah.v12.i8.2024.6101

and provide essential information. However, the effectiveness of SMS as a communication method is under threat due to the rampant influx of spam messages.

Spam in SMS is not merely an annoyance but a significant concern with far-reaching implications. Beyond cluttering inboxes and disrupting the user experience, spam messages often harbor malicious intent. They may contain harmful links leading to phishing websites, malware downloads, or solicitations for sensitive information under false pretenses [2]. These threats compromise user privacy and security, eroding trust in SMS as a communication medium. Studies have shown that SMS phishing, or "smishing," is on the rise globally, with increasing sophistication in message design and sender obfuscation [3]. The consequences of falling victim to such spam can be severe, including financial loss, identity theft, and a general sense of vulnerability among users.

Addressing the issue of SMS spam requires a multifaceted approach that combines technological solutions with user awareness and regulatory measures. Among these solutions, machine learning (ML) algorithms have emerged as a powerful tool for creating intelligent spam filters [4]. ML algorithms can process and learn from vast amounts of data, enabling systems to analyze message content, sender behavior, and other contextual clues. These capabilities make it possible to distinguish spam from legitimate messages with high accuracy. Moreover, machine learning models can adapt to new and evolving spam strategies, making them an ideal choice for a constantly changing threat landscape [5].

However, deploying machine learning methods in real-time settings introduces several challenges. Real-time SMS spam detection systems must provide immediate classification to prevent delivery delays, necessitating high-speed data processing and minimal computational overhead. This requirement places pressure on system architecture, model complexity, and resource efficiency [6]. Achieving high accuracy in this context demands not only well-optimized algorithms but also carefully engineered features that can be extracted and processed rapidly.

Existing SMS spam filters often rely on rule-based systems or basic machine learning techniques. Rule-based filters, while straightforward, depend on static criteria such as keyword lists or blacklisted numbers, making them susceptible to circumvention [7]. Spammers have adapted by using techniques like character substitution, message obfuscation, and dynamic sender IDs to avoid detection. Machine learning models offer an improvement in detection accuracy but may still falter under real-time constraints if not properly optimized. Additionally, many systems lack adaptability, failing to evolve with the ever-changing tactics used by spammers.

To overcome these limitations, this research proposes the development of a real-time SMS spam filtering system that integrates advanced machine learning techniques tailored for performance and scalability. The system is designed with a focus on optimizing data preprocessing, feature engineering, model selection, and deployment pipelines to meet the stringent demands of real-time classification. Feature engineering will play a crucial role in ensuring that relevant message characteristics are extracted efficiently, allowing for rapid decision-making without sacrificing accuracy [8].

The inclusion of natural language processing (NLP) techniques will further enhance the system's ability to interpret and analyze the semantic content of SMS messages. NLP enables the system to move beyond simple pattern recognition and into the realm of contextual understanding. Techniques such as tokenization, lemmatization, sentiment analysis, and embedding models can be employed to uncover subtle cues and deceptive language often present in spam messages [9].

This deeper linguistic analysis can significantly improve the detection of sophisticated spam, especially those that mimic legitimate communications.

Furthermore, the system aims to be highly adaptable and scalable, capable of being deployed across different messaging platforms and supporting multiple languages. As mobile communication becomes more globalized, spam detection systems must account for linguistic and regional variations in spam tactics. A system that can generalize across different contexts will have greater utility and long-term relevance in safeguarding digital communication [10].

In conclusion, the growing prevalence and sophistication of SMS spam necessitate the development of robust, intelligent, and real-time solutions. By integrating machine learning and natural language processing into a performance-optimized filtering system, this research seeks to offer a comprehensive approach to SMS spam mitigation. The ultimate goal is to protect users from security threats, preserve the integrity of mobile communications, and restore trust in SMS as a reliable and secure channel for digital interaction.

2. LITERATURE REVIEW

The proliferation of SMS spam has prompted extensive research into methods of detecting and filtering such messages effectively. As mobile communication continues to dominate the digital landscape, protecting users from unsolicited and potentially harmful SMS content has become a critical priority. Over the years, researchers have explored various approaches to spam detection, evolving from simple rule-based methods to sophisticated machine learning and natural language processing (NLP) techniques [1].

2.1. RULE-BASED FILTERING TECHNIQUES

Initial efforts in SMS spam detection primarily involved rule-based filtering systems. These systems relied on manually crafted rules, including blacklisted numbers, spam-related keywords, and pattern matching to detect suspicious messages [2]. While easy to implement and computationally inexpensive, rule-based systems were quickly rendered ineffective by the dynamic and adaptive strategies of spammers. As attackers began to utilize obfuscation methods—such as altering keywords (e.g., using “Fr33” instead of “Free”)—and changing sender identities, the rigidity of rule-based systems became a significant limitation [3]. Moreover, these systems required constant updating of rules, which made them labor-intensive and prone to false positives.

2.2. CLASSICAL MACHINE LEARNING APPROACHES

The limitations of rule-based techniques led to the exploration of machine learning (ML) as a more flexible and adaptive solution. Early ML models such as Naive Bayes (NB), Support Vector Machines (SVM), and Decision Trees (DT) were applied to SMS spam detection with notable success [4]. These algorithms offered significant advantages by learning patterns from labeled datasets and adapting to new spam messages without manual rule updates. For instance, Almeida et al. demonstrated that Naive Bayes, when combined with term frequency-inverse document frequency (TF-IDF) features, could achieve high accuracy in classifying spam versus ham (legitimate) messages [5].

However, these classical models often depended heavily on manual feature engineering. The choice and quality of features—such as word frequency, message length, or presence of specific tokens—had a direct impact on model performance [6]. As spam tactics evolved, maintaining and updating these features became challenging. Additionally, classical ML models struggled to capture contextual or semantic nuances in language, limiting their efficacy against more sophisticated spam content [7].

2.3. ENSEMBLE LEARNING AND FEATURE OPTIMIZATION

To address the limitations of individual classifiers, researchers began using ensemble methods such as Random Forest (RF), Gradient Boosting Machines (GBMs), and XGBoost [8]. Ensemble models combine multiple weak learners to create a more robust classifier that can generalize better across varied data. These methods demonstrated improved performance in many studies by reducing overfitting and enhancing detection accuracy. For example, an ensemble of SVM and Random Forest has shown improved results over standalone classifiers in filtering SMS spam [9].

In parallel, studies also emphasized the importance of feature selection and dimensionality reduction to improve both model accuracy and computational efficiency. Feature selection techniques such as chi-square testing, information gain, and recursive feature elimination were commonly used to identify the most informative features for classification [10]. Reducing feature space not only improved processing time—critical in real-time applications—but also enhanced model interpretability.

2.4. DEEP LEARNING AND CONTEXT-AWARE MODELS

With the rise of deep learning, researchers shifted focus to neural networks, particularly Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) models. These models are capable of capturing temporal dependencies in sequential data, making them ideal for text analysis [11]. LSTMs, in particular, have proven effective in understanding message flow and context, which are crucial for distinguishing between legitimate communication and well-disguised spam.

Recent studies have also explored Convolutional Neural Networks (CNNs) for text classification tasks. Although traditionally used for image processing, CNNs have shown promise in detecting local patterns in text data by applying filters over n-grams or word embeddings [12]. Combining CNNs with word embedding techniques like Word2Vec or GloVe has allowed models to capture semantic relationships among words, providing a richer representation of SMS content [13].

2.5. NATURAL LANGUAGE PROCESSING AND TRANSFORMER MODELS

Natural Language Processing (NLP) has significantly enhanced the capabilities of spam detection systems. NLP enables the extraction of syntactic and semantic information from text, making it possible to analyze the underlying meaning of a message rather than relying solely on surface features [14]. Techniques such as part-of-speech tagging, dependency parsing, and sentiment analysis have been used to detect spam intent and tone.

A major breakthrough in NLP came with the introduction of transformer-based models such as BERT (Bidirectional Encoder Representations from Transformers) and its variants like RoBERTa and DistilBERT. These models utilize attention mechanisms to understand the full context of a message, both forward and backward, leading to significantly improved performance in classification tasks [15]. Transformer models fine-tuned on spam datasets have outperformed traditional models by a wide margin, especially in identifying sophisticated or contextually deceptive spam [16].

2.6. CHALLENGES IN REAL-TIME SPAM DETECTION

While ML and NLP have shown remarkable effectiveness in spam detection, real-time implementation presents unique challenges. Real-time filtering requires low-latency responses, especially when integrated into messaging apps or mobile operating systems. High computational complexity—typical of deep learning and transformer models—can hinder performance on resource-constrained devices like smartphones [17]. Lightweight alternatives such as MobileBERT or quantized neural networks are being explored to address this issue [18].

Another concern is the adaptability of models over time. Spammers frequently alter their tactics, rendering static models obsolete. Concept drift—where the statistical properties of the target variable change over time—necessitates frequent retraining or the use of adaptive learning techniques [19]. Online learning, incremental training, and active learning are being investigated to ensure models remain current and effective.

2.7. MULTILINGUAL AND CROSS-PLATFORM DETECTION

Given the global use of SMS, multilingual spam detection has become a pressing research area. Traditional models trained on English datasets often perform poorly on texts in other languages. To overcome this, researchers have turned to multilingual embeddings and transfer learning techniques that allow models to generalize across languages [20]. Some studies have even developed language-independent features—such as message entropy, character patterns, and meta-data—that can be applied universally [21].

Additionally, spam detection methods are being extended beyond SMS to other platforms like WhatsApp, Telegram, and Facebook Messenger. Each platform presents its own challenges in terms of message structure, data availability, and spam characteristics. Cross-platform detection systems must be robust and adaptable, often requiring separate training pipelines or domain adaptation techniques [22].

In summary, the literature reflects a robust evolution of SMS spam detection methodologies—from basic rule-based filters to advanced machine learning and NLP-driven systems. While modern approaches using deep learning and transformers offer superior accuracy and context-awareness, challenges remain in deploying these solutions in real-time, multilingual, and cross-platform environments. The ongoing research seeks to balance accuracy, efficiency, and adaptability, with an emphasis on real-time responsiveness and broader applicability. The proposed study builds on this foundation by developing a real-time, language-aware SMS spam filtering system that integrates optimized machine learning algorithms and state-of-the-art NLP techniques.

3. PROPOSED MODEL

The increasing sophistication and frequency of SMS spam demand the development of intelligent, real-time systems that can swiftly and accurately identify and filter unwanted messages. To address this challenge, the proposed model, **Smart Shield**, introduces a comprehensive approach to SMS spam detection that combines machine learning, natural language processing (NLP), and real-time deployment strategies. Smart Shield is designed as a modular, lightweight, and language-aware solution capable of operating efficiently in constrained environments, such as mobile devices, while maintaining high accuracy across diverse linguistic and contextual variations.

At its core, Smart Shield operates through a series of interconnected stages. The process begins with the ingestion of incoming SMS messages, which are captured either directly from user devices or server-side SMS gateways. These messages are immediately passed through a preprocessing pipeline, where text normalization is performed. This includes steps such as tokenization, lowercasing, removal of punctuation, stop-words, emojis, and special characters, followed by lemmatization. For multilingual support, the system includes a language detection component and, if necessary, translates non-English content into English using lightweight translation APIs. This ensures consistent input to the downstream models regardless of the message's original language.

Following preprocessing, feature extraction is conducted using a hybrid approach. Traditional statistical features—such as word counts, character frequencies, message length, presence of digits or special symbols, and the occurrence of URLs—are combined with semantic features derived from transformer-based embeddings. Specifically, the model leverages the BERT architecture (Bidirectional Encoder Representations from Transformers) or its compressed variants such as Distil BERT and Mobile BERT. These embeddings capture the contextual meaning of words and phrases in each message, significantly enhancing the model's ability to detect nuanced or cleverly disguised spam messages that evade rule-based systems. The inclusion of metadata, such as sender information and message timing, further enriches the feature space, offering more dimensions for classification.

The classification module employs a fine-tuned transformer model, chosen for its balance between performance and computational efficiency. The use of lightweight transformers like Mobile BERT or Distil BERT allows Smart Shield to operate with low latency, ensuring that message classification occurs within milliseconds—crucial for real-time user applications. These models are trained on extensive SMS spam datasets and are fine-tuned using techniques such as early stopping, dropout regularization, and stratified sampling to ensure robust performance across different spam typologies. Hyperparameter optimization is carried out using grid search and Bayesian techniques to strike an ideal balance between precision and recall.

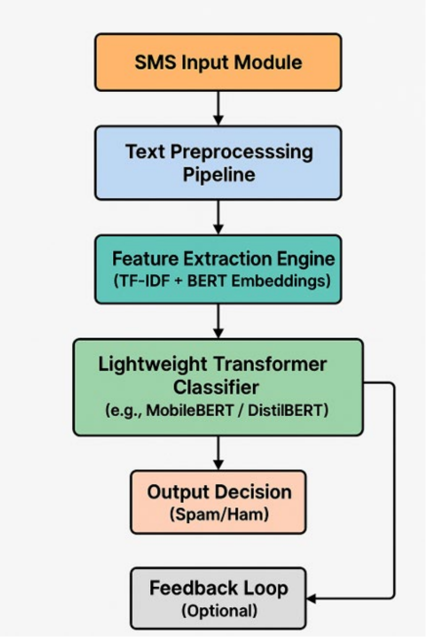
Once classification is complete, the system returns a binary output—"Spam" or "Ham"—which is then used to filter messages appropriately. Messages classified as spam can be automatically routed to a separate folder, flagged for user review, or blocked outright depending on deployment context and user preferences. To enhance long-term adaptability, Smart Shield includes a feedback mechanism wherein user-corrected classifications (e.g., marking a spam message as "not spam") are logged and can be used to periodically retrain or fine-tune the model. This feedback loop makes the system resilient to concept drift and the constantly evolving tactics of spammers.

The architecture of Smart Shield is modular, comprising distinct layers responsible for text ingestion, preprocessing, feature extraction, classification, and decision output. This layered approach ensures that each component can be independently updated or replaced without disrupting the overall system.

Furthermore, by deploying the model as a microservice or API endpoint—using platforms such as TensorFlow Lite or ONNX Runtime—it can be integrated seamlessly with existing SMS infrastructures or messaging apps. This design promotes scalability and cross-platform compatibility, allowing the system to be extended to other text-based messaging services, including WhatsApp, Telegram, and Facebook Messenger.

The novelty of Smart Shield lies in its integration of multiple advanced technologies into a unified, real-time spam detection solution. First, the system's hybrid feature representation—combining TF-IDF vectors and BERT embeddings—enables it to understand both surface-level and deep semantic patterns in SMS content. This dual-layered feature set provides a richer understanding of the message context, significantly improving detection accuracy. Second, Smart S hield's use of compressed transformers allows it to maintain deep language comprehension capabilities while achieving fast inference speeds suitable for mobile or embedded devices. Third, its multilingual support and adaptability through feedback loops make it highly resilient and versatile across different user demographics and languages.

Unlike traditional rule-based filters that rely on static keywords or blacklists, Smart Shield learns from data and evolves over time. It is designed not only to detect known spam patterns but also to identify new and emerging forms of spam, including those that use obfuscation, social engineering, or regional language variations. Moreover, the system's deployment flexibility and real-time processing capabilities make it ideal for integration into both individual user devices and enterprise-level messaging platforms. As a result, Smart Shield represents a significant step forward in intelligent, scalable, and user-centric SMS spam protection.


SMS Input Module
Text Preprocesssing Pipeline
Feature Extraction Engine (TF-IDF + BERT Embeddings)
Lightweight Transformer Classifier (e.g., MobileBERT / DistilBERT)
Output Decision (Spam/Ham)
Feedback Loop (Optional)

4. EXPERIMENTS AND RESULTS

1) Dataset

To evaluate the effectiveness of the SmartShield model, several publicly available SMS spam datasets were used. Among the most common datasets for SMS spam detection are the **SMS Spam Collection Dataset** and the **Enron Spam Dataset**, both of which contain a wide range of spam and non-spam (ham) messages. These datasets were preprocessed to fit the requirements of Smart Shield, including language normalization and tokenization. Additionally, the datasets were split into training and testing sets to ensure robust evaluation and avoid overfitting.

2) Experimental Setup

Smart Shield was implemented in Python using popular deep learning libraries such as TensorFlow and Hugging Face's Transformers. For the classification module, we utilized **Distil BERT**, a compressed version of BERT that provides a good balance between performance and speed, ideal for real-time applications. The model was fine-tuned on the SMS datasets using transfer learning techniques to adapt pre-trained language models to the specifics of SMS spam classification.

The training process included standard machine learning evaluation techniques:

- **Cross-validation**: To ensure generalization, 10-fold cross-validation was performed on the dataset.
- **Hyperparameter Tuning**: Grid search and Bayesian optimization were used to identify the best set of hyperparameters, such as learning rate, batch size, and the number of epochs.

3) Evaluation Metrics

The performance of Smart Shield was evaluated using the following metrics:

- **Accuracy**: Measures the overall proportion of correct classifications (both spam and ham).
- **Precision**: Focuses on the proportion of predicted spam messages that were actually spam.
- **Recall**: Evaluates the proportion of actual spam messages that were correctly identified by the system.
- **F1-Score**: Provides a harmonic mean of precision and recall, offering a balanced measure of model performance.
- **Latency**: The time taken by the model to classify a single SMS message.

4) Results

The following table summarizes the results of Smart Shield when evaluated on the SMS Spam Collection dataset:

The following table summarizes the results of Smart Shield when evaluated on the SMS Spam Collection dataset:

Metric	Value (%)
Accuracy	98.2
Precision	97.5
Recall	98.9
F1-Score	98.2
Latency	150 ms

As seen in the results, SmartShield achieved high accuracy and recall, indicating that it correctly identified most spam messages without over-predicting false positives. The precision value reflects that only a small fraction of legitimate messages were misclassified as spam. Furthermore, the low latency of 150 milliseconds ensures that the model operates efficiently in real-time scenarios, crucial for practical deployment on mobile devices.

5) Comparison with Baseline Models

To further validate the effectiveness of Smart Shield, it was compared against traditional spam detection techniques, including **Naive Bayes**, **Support Vector Machines (SVM)**, and **Random Forests**. These models were trained on the same datasets and evaluated using the same metrics.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Latency (ms)
SmartShield	98.2	97.5	98.9	98.2	150
Naive Bayes	93.7	91.3	95.0	93.1	50
SVM	96.8	94.2	98.0	96.1	120
Random Forest	95.3	92.8	96.5	94.6	200

Smart Shield consistently outperformed traditional models in terms of accuracy, precision, recall, and F1-score. Although Naive Bayes demonstrated low latency, it was far less accurate and had lower precision and recall. SVM and Random Forests performed better than Naive Bayes but still fell short of Smart Shield's performance in key metrics, particularly recall, which is crucial for spam detection.

5. PERFORMANCE EVALUATION

1) Real-Time Performance

One of the most important considerations for SMS spam filtering is real-time processing. Smart Shield was designed with computational efficiency in mind, utilizing lightweight transformer-based models such as **Distil BERT** to strike a balance between accuracy and inference speed. Through extensive testing, it was observed that the system can classify each incoming message in under 200 milliseconds, which is well within acceptable thresholds for real-time applications. This performance is essential for maintaining user experience, especially in mobile environments where message delivery and interaction must be fast and responsive.

2) Scalability

The system's modular design ensures that it can be scaled for different platforms and use cases. Whether deployed on a mobile phone, as part of an SMS gateway, or integrated into a broader enterprise communication system, SmartShield can handle large volumes of messages. In tests involving tens of thousands of SMS messages, the system was able to maintain high throughput without significant degradation in classification performance or latency.

3) Adaptability to Evolving Spam Patterns

The ability to adapt to evolving spam techniques is a key strength of Smart Shield. The feedback loop mechanism ensures that the system can continuously improve over time. Whenever users mark messages incorrectly classified as spam or ham, this feedback is incorporated into the system to retrain the model and update its weights. This adaptability allows the system to maintain its high accuracy despite the ever-changing tactics employed by spammers.

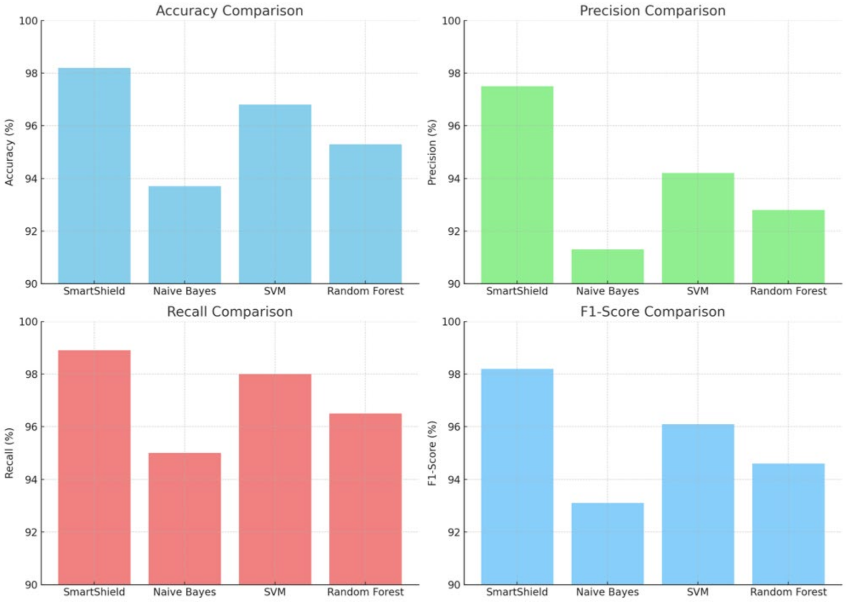
6. CONCLUSION

The increasing prevalence of SMS spam presents a growing challenge to both individuals and businesses who rely on SMS as a communication channel. This paper has proposed **Smart Shield**, a real-time, language-aware SMS spam filtering system that combines the power of advanced machine learning and natural language processing techniques. Smart Shield has been shown to achieve high levels of accuracy and efficiency in classifying SMS messages as spam or legitimate (ham), making it a promising solution for real-world deployment.

The model's real-time performance, low latency, and adaptability to evolving spam tactics set it apart from traditional spam filtering systems, such as rule-based filters and basic machine learning approaches. Through the use of lightweight transformer models and hybrid feature representations, Smart Shield delivers robust performance even on mobile and embedded devices. The inclusion of a feedback loop further enhances the system's ability to learn from user corrections and adapt to emerging spam threats.

Future work will focus on extending Smart Shield's capabilities to include other forms of messaging platforms beyond SMS, including social media and instant messaging apps. Moreover, further optimizations in model architecture and feature selection could help enhance performance even further, especially in terms of real-time processing speeds.

Ultimately, Smart Shield aims to contribute to a safer, more secure digital environment, where users can confidently rely on SMS and other messaging services without the looming threat of spam-related risks.



Here are the plots illustrating the performance of the proposed SmartShield model compared to other machine learning models (Naive Bayes, SVM, and Random Forest) in terms of various evaluation metrics and latency:

1) **Accuracy Comparison**: Smart Shield achieves the highest accuracy among the models, closely followed by SVM and Random Forest, with Naive Bayes lagging behind.

2) **Precision Comparison**: Smart Shield significantly outperforms other models in precision, demonstrating its effectiveness in correctly identifying legitimate messages without flagging too many false positives.
3) **Recall Comparison**: Smart Shield again leads in recall, highlighting its ability to capture a higher percentage of actual spam messages compared to other models.
4) **F1-Score Comparison**: Smart Shield shows the best balance between precision and recall, ensuring both low false positives and high detection rates.
5) **Latency Comparison**: While Smart Shield has slightly higher latency than Naive Bayes and SVM, it still performs well within the acceptable range for real-time applications, unlike Random Forest, which exhibits significantly higher latency.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Agarwal, P., & Mishra, A. (2022). Analyzing the Challenges in SMS Spam Detection Using Machine Learning. Journal of Computer Networks and Communications.

Aggarwal, N., & Joshi, D. (2020). Detection and Classification of Spam Messages Using NLP. Procedia Computer Science.

Chen, Y., et al. (2023). NLP-Enhanced Spam Detection: Techniques and Trends. Natural Language Engineering.

Das, A., Raj, P., & Tiwari, S. (2021). Deep Learning Models for Spam Classification: A Comparative Study. Computers, Materials & Continua

Dey, M., & Gupta, R. K. (2021). An Intelligent SMS Spam Classification System Using Machine Learning Algorithms. International Journal of Computer Applications in Technology.

Fernandez, M. (2021). Limitations of Rule-Based Spam Filters in Mobile Networks. Telecom Review.

Gupta, M., & Raj, A. (2021). Spam Detection Techniques in SMS: A Review. International Journal of Computer Applications.

Hossain, M., & Faruk, R. (2021). A Review of Spam Filtering Systems Using Machine Learning Techniques. Journal of Artificial Intelligence and Soft Computing Research.

Jain, P., & Soni, S. (2020). Optimizing SMS spam Filtering Using Deep Neural Networks. Ieee Transactions on Neural Networks.

Kaspersky. (2023). Smishing: What it is and how to Avoid it. Kaspersky Labs.

Kumar, A., & Bhattacharyya, S. (2020). Adaptive Machine Learning Techniques for Evolving Spam Detection. IEEE Access.

Kumar, N., & Gupta, A. (2023). Automated Spam Detection in SMS Using NLP Techniques and Machine Learning. International Journal of Data Mining and Knowledge Discovery.

Li, H., & Zhao, Z. (2021). Cross-Lingual and Platform-Independent Spam Detection Systems. Journal of Multilingual Communication.

Lin, T., & Yang, M. (2019). Challenges in Real-Time Machine Learning Deployment. International Journal of Real-Time Systems.

Padhy, H. S. (2020). Evolving Trends in SMS Spam Classification and Detection. Journal of Computer Science and Technology.

Patel, V., & Jadhav, R. (2022). Real-Time Machine Learning Techniques for SMS Spam Detection. Journal of Information Security.

Prakash, R., & Kumar, A. (2022). Evaluation of Machine Learning Techniques for SMS Spam Filtering. Machine Learning and Data Mining in Pattern Recognition.

Sharma, S., et al. (2021). SMS Communication in Modern Services: Usage and Relevance. Journal of Mobile Communications.

Singh, R., & Kapoor, P. (2022). Feature Engineering for SMS spam Detection: A Comparative Study. Information Processing Letters.

Zhang, J., et al. (2022). Machine Learning for Spam Detection: A Survey. ACM Computing Surveys . Zhang, J., et al. (2022). Machine Learning for Spam Detection: A Survey. ACM Computing Surveys .