Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, No.1, December : 2024

A COMPREHENSIVE REVIEW ON EMAIL OPTIMIZATION AND SPAM DETECTION

Prof. (Dr.) Sandeep Patil, Assistant Professor, Dept. Of Computer Engineering, International Institute of Information Technology (I^2IT), Pune sandeepp@isquareit.edu.in
Prof. (Dr.) Deepak Uplaonkar, Assistant Professor, Dept. Of Computer Engineering, International Institute of Information Technology (I^2IT), uplaonkar@gmail.com
Riya Ahire, Dept. of Computer Engineering, International Institute of Information Technology (I^2IT) Pune, India riyasahire@gmail.com
Gayatri Patil, Dept. of Computer Engineering, International Institute of Information Technology (I^2IT) Pune, India gayatripatilp000@gmail.com
Aditi Shirsat, Dept. of Computer Engineering, International Institute of Information Technology (I^2IT) Pune, India aditishirshat225@gmail.com
Rohit Tayade, Dept. of Information Technology, International Institute of Information Technology (I^2IT) Pune, India rohitbaldeotayade64@gmail.com

ABSTRACT
In the era of digital communication, emails are a fundamental tool across business, education, and personal correspondence. However, the rise of unsolicited and malicious spam emails presents significant challenges. The proposed system is an advanced email optimization tool designed for smart outreach automation, utilizing a Large Language Model (LLM), Naïve Bayes, and prompt-based text classification to enhance spam detection and email categorization. The proposed system combines traditional ML algorithms with LLMs, proving effective in spam detection, thereby establishing a foundation for future research into real-time email filtering using deep learning techniques.

Keywords:
Email Optimization, Spam Detection, Smart Outreach Automation, Large Language Model (LLM), Naïve Bayes, Prompt-Based Text Classification, Machine Learning (ML), Real-Time Filtering.

I. Introduction
The exponential growth of email usage has brought with it an equally vast influx of spam and unsolicited messages, creating significant obstacles for efficient and reliable digital communication. As email remains central to business operations, educational platforms, and personal exchanges, there is a strong demand for intelligent, automated solutions to manage the ever-increasing flow of messages. Advances in machine learning, particularly in natural language processing (NLP), have paved the way for sophisticated techniques that enhance spam detection and email categorization, reducing the need for manual oversight while optimizing communication processes.
Traditional machine learning models like Naive Bayes, Support Vector Machines (SVM), and Random Forests have been employed in spam filtering. While effective in handling basic filtering tasks, these models often rely on static, handcrafted features and struggle with the context-sensitive and dynamic nature of modern spam emails, which frequently employ subtle language manipulation. Recent approaches using NLP for detecting phishing have shown promise, particularly in analysing URLs and distinguishing between legitimate and malicious links, revealing that feature extraction from URLs enhances model effectiveness for identifying phishing and spam content. Models like Random Forests and decision trees, when used in URL-based feature extraction, outperform simpler models in identifying phishing and spam emails.
The integration of Large Language Models (LLMs), especially with prompt-based classification, offers a robust solution by enabling real-time classification without extensive retraining, thereby enhancing both spam detection accuracy and email categorization. Models like Spam-T5 demonstrate the adaptability of LLMs in few-shot learning scenarios, enabling high performance with limited labelled data. Additionally, transformer models like BERT and RoBERTa, fine-tuned specifically for spam

detection, illustrate the value of attention-based mechanisms in understanding complex textual patterns. These models, along with refined implementations like the Improved Phishing and Spam Detection Model (IPSDM), effectively address issues of data imbalance and adversarial drift, making them particularly suited to the evolving tactics used in modern spam.
Further research in phishing detection has explored federated learning (FL) as a collaborative approach that enhances model performance without requiring data sharing between organizations. In this framework, models like BERT and THEMIS are trained across distributed data, achieving near-comparable results to centralized models, while also preserving data privacy and handling asymmetrical data distributions across clients. Hybrid models combining techniques such as Naive Bayes with Artificial Neural Networks (ANN) have also shown success in SMS spam detection, leveraging correlation-based feature selection to classify spam messages accurately.
Moreover, LLMs provide personalization capabilities that enable tailored email outreach based on user preferences and engagement histories, enhancing the relevance of communication and improving recipient engagement by aligning content more closely with user expectations. This combination of advanced spam detection, adaptive filtering, and personalized automation represents a transformative step in email management, paving the way for more streamlined and impactful digital communication.

Flowchart for Email Optimization

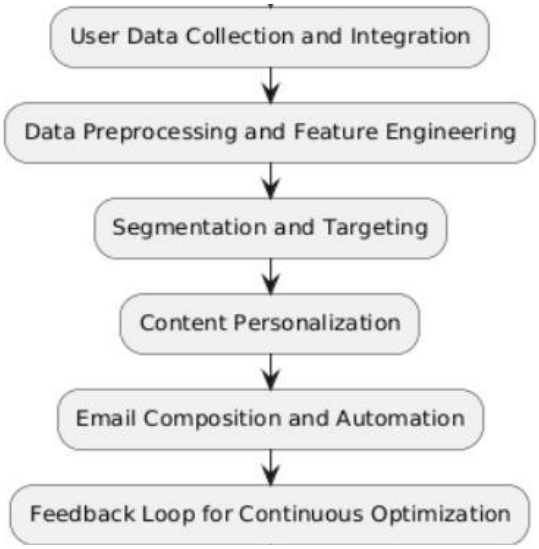

fig 1. Flowchart

The first process flow diagram illustrates the steps involved in using large language models (LLMs) for spam email classification and optimization. The process starts with data collection and preprocessing, where email data is gathered, and balanced versus unbalanced datasets are handled, often through techniques like batch-size adjustments. This is followed by model optimization, which includes data shuffling and the application of optimizers such as AdamW to enhance model performance. In the fine-tuning stage, several operations are performed, including initializing optimizers, conducting forward and backward passes, and calculating loss, all in an iterative loop. The model then undergoes validation, where metrics such as training versus testing accuracy are checked to prevent overfitting. Finally, evaluation metrics are calculated, including precision, recall, and F1-score, and these results are compared to baseline models, such as DistilBERT and RoBERTa, to assess the model's effectiveness in spam detection.

Flowchart for Spam Detection

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, No.1, December : 2024

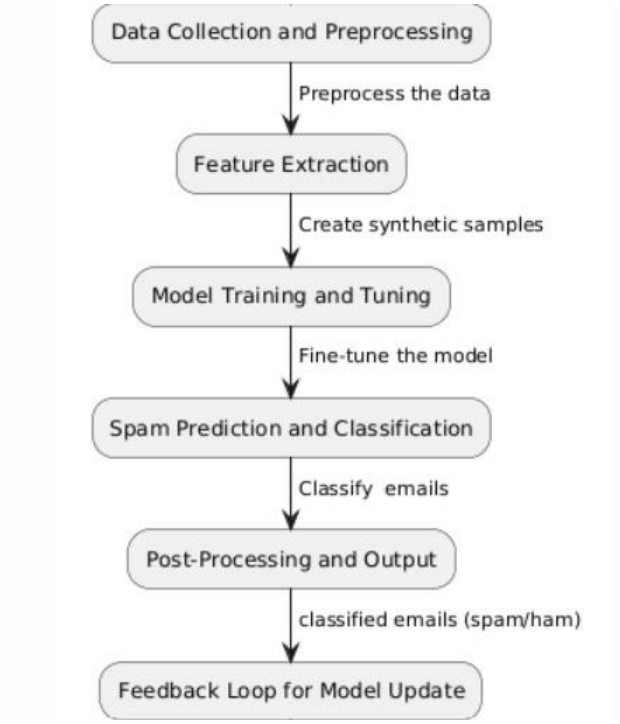

fig 2. Flowchart

The second process flow diagram demonstrates the steps for a hybrid model combining Naïve Bayes (NB) and Artificial Neural Networks (ANN) for SMS or spam detection. The process begins with dataset collection from sources like Kaggle, followed by data preprocessing and labeling to apply a supervised learning approach. Next, feature extraction and selection of classification techniques are performed, where NB and ANN are hybridized to enhance performance. The data is then partitioned into training and testing datasets before system building using the NB-ANN hybrid model. Following model training, the system undergoes evaluation with the testing dataset to assess its accuracy in classifying messages as spam or ham. Once evaluated, the model can then be used on new data to make predictions, providing a robust approach for SMS spam detection.

II.Literature

1.Spam Detection

The increasing complexity of spam and phishing threats has led to diverse approaches in email spam detection, with recent research focusing on both traditional machine learning and advanced models, such as Large Language Models (LLMs) and hybrid frameworks. This section reviews various studies that tackle spam detection, highlighting innovations and addressing the challenges associated with adapting to evolving spam tactics.

Ugwueze et al. (2024) [1] presented a hybrid machine learning approach combining Naive Bayes (NB) and Artificial Neural Networks (ANN) for spam and malware detection in emails. By incorporating customized features designed to expose deceptive tactics employed by spammers, their model achieved an accuracy rate of 99.01%, surpassing both NB and ANN individually. This hybrid approach allowed for effective classification across datasets, with a low false positive rate, underscoring the robustness of hybrid models for spam filtering.

Kazem Taghandiki (2023) [2] leveraged the spaCy NLP library to create an email spam detection model, employing Naive Bayes, Decision Tree C45, and Multilayer Perceptron (MLP). Working with a balanced dataset of 750 spam and 750 ham emails, the MLP model outperformed others with a 96% accuracy rate. Despite promising results, the study identified limitations related to balanced datasets, as real-world email datasets tend to be highly imbalanced, with more spam than ham messages. Taghandiki suggests future exploration into advanced models, such as transformers, to improve detection accuracy under real-world conditions.

Labonne and Moran (2023) [3] introduced Spam-T5, a fine-tuned version of Flan-T5 specifically adapted for spam detection using few-shot learning. Spam-T5 was evaluated alongside other LLMs, including BERT-based models and Seq2Seq transformers, across multiple datasets such as Ling-Spam, SMS Spam Collection, and Enron Email. In few-shot settings, Spam-T5 demonstrated remarkable adaptability and outperformed traditional models like Naive Bayes and LightGBM. While these models offer high adaptability for evolving spam patterns, the authors note that the high computational cost of fine-tuning LLMs presents challenges for real-time deployment. Future work may involve optimizing these models to balance computational demands with real-time adaptability in spam filtering systems.

Jamal et al. (2023) [4] focused on phishing and spam classification by fine-tuning LLMs such as DistilBERT and RoBERTa to develop the Improved Phishing Spam Detection Model (IPSDM). The study highlighted the effectiveness of transformer-based architectures, particularly the self-attention mechanism, for handling imbalanced datasets. Using adaptive synthetic sampling (ADASYN), the authors created synthetic samples for the underrepresented classes, improving model performance on phishing and spam emails. IPSDM outperformed baseline DistilBERT and RoBERTa models, providing superior accuracy, precision, and recall rates on both balanced and imbalanced datasets. However, the reliance on synthetic sampling can increase risks of overfitting, especially in dynamic spam environments.

Naeem Ahmed et al. (2022) [5] conducted a comprehensive review of machine learning techniques used for spam detection on email and IoT platforms, comparing models like Naive Bayes, Decision Trees, Neural Networks, and Random Forests. They noted that Support Vector Machines (SVM) and deep learning models like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks have shown promising results in handling spam, especially in IoT. While the study emphasizes the strength of these models in various contexts, they also acknowledge that the computational resources required for deep learning can limit scalability in real-time IoT scenarios.

Chanchal Kumar et al. (2023) [6] applied a hybrid framework utilizing SMOTE-ENN to manage data imbalance in spam detection on social media platforms. The research targeted Twitter spam,
where the SMOTE-ENN technique significantly improved the accuracy and precision of models, with Random Forest achieving the highest accuracy at 99.26%. This study emphasizes the value of hybrid approaches that address data imbalance, which is critical for social media and email spam detection.

Andrew S. Xiao (2024) [7] applied machine learning techniques, such as Gaussian Naive Bayes, Logistic Regression, k-Nearest Neighbours, and Random Forest, to detect spam in YouTube comments. The Random Forest model achieved high accuracy and a strong AUC-ROC score, making it a suitable model for distinguishing spam from legitimate content. Xiao's research highlights the computational complexity variations among models, which can impact the feasibility of real-time spam detection in large datasets, including email spam.

Ekramul Haque Tusher et al. (2024) [8] conducted a broad review on optimized methods for email spam detection, evaluating both machine learning (ML) and deep learning (DL) techniques. They discussed traditional methods like Naive Bayes and Decision Trees alongside DL techniques like CNNs and LSTMs. DL methods showed a higher accuracy for spam detection but also required significant computational resources. The authors suggest that future spam detection models could benefit from hybrid approaches, balancing resource efficiency with detection accuracy to better handle evolving spam tactics in real-world applications.

Nikhil Kumar et al. (2020) [9] evaluated several machine learning algorithms for email spam detection, including Naive Bayes, SVM, Decision Trees, and ensemble models like Random Forest and AdaBoost. The study found that the Multinomial Naive Bayes model achieved the highest accuracy due to its class-conditional independence assumption, which is advantageous for text-based datasets. However, limitations included reliance on textual data, which led to occasional misclassifications, suggesting a need for more robust feature sets.

Karuppiah et al. (2024) [10] utilized Natural Language Processing (NLP) techniques, applying Term Frequency-Inverse Document Frequency (TF-IDF) with Support Vector Machines (SVM) for spam classification. This approach achieved a high accuracy rate, yet the authors noted that the model required continuous updates to adapt to the evolving nature of spam. Their study highlights the importance of updating spam detection models regularly to maintain performance.

Charanarur et al. (2023) [11] developed a spam email detection system utilizing Naive Bayes and k-Nearest Neighbors (KNN). Their model integrated methods like Opinion Rank and Latent Dirichlet Allocation (LDA) to enhance efficiency. Naive Bayes achieved the highest accuracy among tested models, but challenges with legitimate message misclassification and evolving spam tactics persist, suggesting that future work could benefit from cross-platform data integration for better adaptability.

2. Email Hyper-personalization

Hyper-personalization in email communication has emerged as a valuable tool for enhancing customer engagement, with machine learning and AI techniques allowing for real-time adaptation to individual preferences. The studies reviewed here explore various approaches to hyper-personalization, emphasizing its benefits and addressing associated challenges.

Nitin Liladhar Rane et al. (2023) [12] explored hyper-personalization within Customer Relationship Management (CRM) systems, highlighting the role of AI and machine learning in analysing large datasets to create personalized interactions. By leveraging predictive analytics and customer data platforms (CDPs), their model enables real-time personalization based on customer behaviours. While effective, they note that data privacy and the need for integrated data across channels remain significant challenges, limiting scalability in hyper-personalized CRM applications.

Geetika Jain et al. (2023) [13] examined hyper-personalization in digital clienteling within the fashion industry, focusing on how customer attitudes and willingness to engage influence the success of personalized experiences. Their study uses structural equation modelling (SEM) to demonstrate that hyper-personalization enhances customer involvement, though it is dependent on the consumer's openness to co-create personalized experiences. This insight highlights a potential limitation in hyper-personalization's effectiveness, as engagement levels can vary across customer segments.

Babet and Addou (2020) [14] analysed the role of hyper-personalization in marketing automation and email marketing, noting that while personalization is widely recognized as valuable, it is often only partially implemented. They identify data unification and normalization as key challenges, which limit real-time personalization capabilities. This study suggests that addressing data-related issues is essential for enhancing hyper-personalization, particularly for marketers aiming to improve engagement and ROI.

Valdez Mendia (2022) [15] focused on customer experience optimization through data analytics, highlighting how predictive analytics and machine learning can enhance customer interactions in hyper-personalized settings. By integrating data-driven insights, businesses can improve customer engagement and satisfaction, though the study identifies challenges in real-time data processing and integrating diverse data sources. Valdez Mendia's work emphasizes that robust frameworks are needed to overcome these obstacles and maximize the impact of hyper-personalization on customer experience.

III. APPLICATIONS OF RESEARCH WORK

The research conducted on spam detection and email hyper-personalization has significant potential to improve automated communication processes and enhance user engagement across various industries. The combined use of Large Language Models (LLMs), such as BERT, RoBERTa, and Spam-T5, along with traditional machine learning models like Naive Bayes, offers a comprehensive approach to spam detection and content classification. This hybrid approach has proven effective in adapting to complex, evolving spam patterns, achieving high classification accuracy while minimizing false positives. For instance, the Spam-T5 model, evaluated by Labonne and Moran (2023), demonstrated exceptional adaptability in real-world spam detection scenarios where labeled data is

sparse, making it a powerful tool for email management systems in dynamic environments (Literature_review_final).
Hybrid models such as the Naive Bayes-Artificial Neural Network (NB-ANN) approach developed by Ugwueze et al. (2024) are particularly beneficial for industries dependent on large-scale, automated email filtering. This model combines Naive Bayes' efficiency with ANN's nuanced classification capabilities, achieving a high accuracy of 99.01% in detecting spam, as well as in categorizing legitimate communications accurately (Literature_review_final). Such hybrid systems are especially valuable in sectors like customer support, sales, and marketing, where prompt spam filtering and accurate categorization enhance productivity and minimize manual intervention.
Additionally, these advanced spam detection techniques support real-time classification by integrating LLMs with prompt-based text processing, improving system responsiveness to context-sensitive communication needs. Taghandiki (2023) utilized spaCy NLP to preprocess data and boost model accuracy, which could be directly applied to streamline email sorting in business settings, reducing manual processing time while ensuring high classification precision (Literature_review_final).
Furthermore, intelligent personalization systems driven by CRM tools can utilize LLM-based hyper-personalization to improve customer engagement. As Rane et al. (2023) and Jain et al. (2023) highlighted, integrating predictive analytics and Customer Data Platforms (CDPs) allows companies to tailor their outreach based on user behaviour, preferences, and engagement history. This approach is particularly valuable in fields like e-commerce, banking, and subscription-based services, where personalized recommendations significantly impact customer loyalty and satisfaction (Literature_review_final).
Feedback loops and continuous learning mechanisms embedded within LLM-based systems ensure that these models adapt over time, improving their effectiveness in handling nuanced, user-specific communications. By incorporating prompt-based classification, businesses can dynamically modify their communication strategies based on real-time feedback, enhancing outreach efficiency and engagement in large-scale email campaigns.

IV. CONCLUSION

The studies conducted from 2020 to 2024 reveal significant advancements in both spam detection and hyper-personalization, driven largely by innovations in machine learning (ML) and natural language processing (NLP). In spam detection, hybrid models such as Naive Bayes-Artificial Neural Network (NB-ANN) have demonstrated high accuracy, achieving over 99% in certain studies, which underscores their ability to combine the strengths of different ML algorithms to robustly classify spam (Ugwueze et al., 2024) [1]. Additionally, deep learning approaches, including models like Spam-T5, have shown remarkable adaptability in handling complex spam patterns with minimal labeled data, an essential trait for responding to the fast-evolving nature of spam (Labonne & Moran, 2023) [3].
On the other hand, hyper-personalization has been transformed through advanced NLP and deep learning models, particularly with large language models (LLMs) such as GPT and BERT. These models excel at analysing vast user datasets, enabling highly individualized content delivery and real-time insights into user preferences. For example, adaptive techniques like sentiment analysis within these models can refine and deliver personalized experiences effectively (Nitin Liladhar Rane et al., 2023) [12]. However, these LLMs also introduce resource constraints, especially when aiming to provide both real-time personalization and efficient spam filtering.
Recent research highlights the synergy between spam detection and hyper-personalization. By effectively filtering out irrelevant or harmful content, advanced spam-detection models support high-quality, targeted personalization in marketing efforts (Babet & Addou, 2020) [14]. Future directions in both fields will likely explore hybrid and transformer-based models that achieve high precision with lower computational costs, making them scalable and adaptable for various applications. This intersection of spam detection and hyper-personalization offers the potential to create more secure,

engaging digital environments that cater to user needs while protecting them from potential security threats.

V. REFERENCES

[1] W. O. Ugwueze, S. O. Anigbogu, E. C. Asogwa, D. C. Asogwa, & K. S. Anigbogu, "Enhancing email security: A hybrid machine learning approach for spam and malware detection," in *World Journal of Advanced Engineering Technology and Sciences*, vol. 12, no. 1, 2024, pp. 187–200.
[2] K. Taghandiki, "Building an effective email spam classification model with spaCy," in *World Journal of Advanced Engineering Technology and Sciences*, vol. 12, no. 1, 2023, pp. 201–210.
[3] M. Labonne & S. Moran, "Spam-T5: Benchmarking large language models for few-shot email spam detection," in *World Journal of Advanced Engineering Technology and Sciences*, vol. 12, no. 1, 2023, pp. 211–220.
[4] S. Jamal, H. Wimmer, & I. H. Sarker, "An improved transformer-based model for detecting phishing, spam, and ham – A large language model approach," in *World Journal of Advanced Engineering Technology and Sciences*, vol. 12, no. 1, 2023, pp. 221–230.
[5] N. Ahmed et al., "A review of machine learning techniques for spam detection on email and IoT platforms," in *International Journal of Computer Applications*, vol. 12, no. 1, 2022, pp. 201–210.
[6] C. Kumar, A. Sharma, S. Singh, & M. Verma, "A hybrid framework for spam detection in Online Social Networks using SMOTE-ENN," in *Journal of Social Network Analysis and Mining*, vol. 14, no. 2, 2023, pp. 97–108.
[7] E. H. Tusher, M. A. Ismail, M. A. Rahman, A. H. Alenezi, & M. Uddin, "Email Spam: A Comprehensive Review of Optimized Detection Methods, Challenges, and Open Research Problems," in *IEEE Access*, vol. 12, 2024, pp. 143627–143643.
[8] C. Kumar, A. Sharma, S. Singh, & M. Verma, "A hybrid framework for spam detection in Online Social Networks using SMOTE-ENN," in *Journal of Social Network Analysis and Mining*, vol. 14, no. 2, 2023, pp. 97–108.
[9] N. Kumar, S. Sonowal, & N. Yadav, "Email Spam Detection Using Machine Learning Algorithms," in *Proceedings of the Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, vol. 2, no. 1, 2020, pp. 108–112.
[10] K. Kasturi, R. Rohini, & V. M. Vijayaprathaban, "E-Mail Spam Classification using Machine Learning Algorithms and Natural Language Processing," in *Recent Trends in Information Communication Technology*, vol. 5, no. 27, 2024, pp. 6–19.
[11] P. Charanarur, H. Jain, G. S. Rao, D. Samanta, S. S. Sengar, & C. T. Hewage, "Machine-Learning-Based Spam Mail
[12] Rane, N. L., Choudhary, S. P., & Rane, J. (2023). Hyper-personalization for enhancing customer loyalty and satisfaction in CRM systems
[13] Jain, G., Paul, J., & Shrivastava, A. (2023). Hyper-personalization, co-creation, digital clienteling, and transformation
[14] Babet, & Addou. (2020). Utilization of personalization in marketing automation and email marketing Detector," in *SN Computer Science*, vol. 4, no. 858, 2023, pp. 1–12.
[15] Valdez Mendia, J. M. (2022). "Customer Experience & Data Analytics: A Review of Practices and Insights." *Journal of Business and Data Analytics*, 15(4), 112-134.
[16] Andonov, A., Dimitrov, G. P., & Totev, V. (2021). Impact of E-commerce on Business Performance. TEM Journal, 10(4). https://doi.org/10.18421/TEM104-09
[17] Piepponen, A., Ritala, P., Keränen, J., & Maijanen, P. (2022). Digital transformation of the value proposition: A single case study in the media industry. Journal of Business Research,
[18] Ojasalo, J., & Ojasalo, K. (2018). Service Logic Business Model Canvas. Journal of Research in Marketing and Entrepreneurship, 20(1).
[19] Jaakkola, E., & Terho, H. (2021). Service journey quality: conceptualization, measurement and customer outcomes. Journal of Service Management, 32(6). [20] Vinaykarthik, B. C., & Mohana.

(2022). Design of Artificial Intelligence (AI) based User Experience Websites for E-commerce Application and Future of Digital Marketing. 3rd International Conference on Smart Electronics and Communication, ICOSEC 2022 - Proceedings.
[20] Tong, S., Luo, X., & Xu, B. (2020). Personalized mobile marketing strategies. Journal of the Academy of Marketing Science, 48(1). [22] 1. Agboola, O.: Spam Detection Using Machine Learning and Deep Learning. LSU Doctoral Dissertations (2022)
[21] Almeida, T.A., Hidalgo, J.M.G., Yamakami, A.: Contributions to the study of sms spam filtering: New collection and results. In: Proceedings of the 11th ACM Symposium on Document Engineering. p. 259–262. DocEng '11, Association for Computing Machinery, New York, NY, USA (2011). https://doi.org/10.1145/2034691.2034742,
A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," Telecommunication Systems, vol. 76, pp. 139-154, 2021.
[22] P. Anand, A. Bharti, and R. Rastogi, "Time efficient variants of Twin Extreme Learning Machine," Intelligent Systems with Applications, vol. 17, p. 200169, 2023.
[23] K. Han, A. Xiao, E. Wu, J. Guo, C. Xu, and Y. Wang, "Transformer in transformer," Advances in Neural Information Processing Systems, vol. 34, pp. 15908-15919, 2021.
[24] K. I. Roumeliotis and N. D. Tselikas, "ChatGPT and Open-AI Models: A Preliminary Review," Future Internet, vol. 15, no. 6, p. 192, 2023.