Iraqi Journal for Computer Science and Mathematics

Volume 6 | Issue 1 Article 2

2025

# Email Spam Classification Based on Deep Learning Methods: A Review

Ekramul Haque Tusher
*Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, 26600, Pekan, Malaysia*

Mohd Arfian Ismail
*Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, 26600, Pekan, Malaysia AND Center of Excellence for Artificial Intelligence & Data Science, Universiti Malaysia Pahang Al-Sultan Abdullah, Lebuhraya Tun Razak, Gambang 26300, Malaysia*, arfian@umpsa.edu.my

Anis Farihan Mat Raffei
*Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, 26600, Pekan, Malaysia*



## Recommended Citation

Tusher, Ekramul Haque; Ismail, Mohd Arfian; and Mat Raffei, Anis Farihan (2025) "Email Spam Classification Based on Deep Learning Methods: A Review," *Iraqi Journal for Computer Science and Mathematics*: Vol. 6: Iss. 1, Article 2.
DOI: https://doi.org/10.52866/2788-7421.1236
Available at: https://ijcsm.researchcommons.org/ijcsm/vol6/iss1/2

IRAQI JOURNAL FOR COMPUTER SCIENCE AND MATHEMATICS 2025;6:24–36



REVIEW

# Email Spam Classification Based on Deep Learning Methods: A Review

**Ekramul Haque Tusher** [a], **Mohd Arfian Ismail** [a,b,*], **Anis Farihan Mat Raffei** [a]

[a] Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, 26600, Pekan, Malaysia
[b] Center of Excellence for Artificial Intelligence & Data Science, Universiti Malaysia Pahang Al-Sultan Abdullah, Lebuhraya Tun Razak, Gambang 26300, Malaysia

## ABSTRACT

Email spam is a significant issue confronting both email consumers and providers. The evolution of spam filtering has progressed considerably, transitioning from basic rule-based filters to more sophisticated machine learning algorithms. Deep learning has become a potent collection of techniques for addressing intricate issues such as spam classification in recent times. A thorough literature evaluation is required to have a comprehensive overview of the current research on utilizing deep learning methods for email spam classification. This review aims to identify the various deep learning techniques used for email spam, their effectiveness, and areas for future research. By synthesizing the outcomes of pertinent studies, this review delineates the strengths and drawbacks of various approaches, offering valuable insights into the challenges that must be tackled to enhance the precision and efficacy of email spam classification.

**Keywords:** Email spam, Deep learning, Classification

## 1. Introduction

Email has become the predominant mode of communication for most internet users. However, over the past few years, the growing usage of email has given rise to the serious problem of spam emails. Defined as bulk unsolicited messages, spam or junk email now makes up over 50% of total email traffic by some estimates. An average user receives around 40–50 emails daily, many of which are spam. Spammers earn nearly $3.5 million USD annually from spam, draining productivity for individuals and imposing financial losses on institutions [1]. Users spend precious time sifting through these unproductive communications. Beyond mere nuisance, spam enables more damaging cybercrimes. Spammers frequently have malicious objectives including identity theft, financial fraud, data theft, and reputation harm. To achieve such ends, spam often contains phishing links, embedded malware and perpetuates scams. The massive volume of spam also strains email infrastructure like servers and networks [2]. In light of these threats, effective management and filtration of spam has become a crucial need. Automatically detecting and classifying spam from ham (legitimate email) can boost organizational productivity while reducing costs incurred by spam [3, 4]. Mitigating spam also alleviates downstream cyber risks to assets like customer data, intellectual property, and bank accounts.

Spam filtering seeks to automatically detect and block unwanted spam messages. The first spam filters relied on simple rule-based approaches that looked for obvious red flags in the email header and content. These proved inadequate against the constant evolution of tricks used by spammers to disguise their emails as legitimate [5]. Modern machine learning techniques have enabled more robust statistical spam detection based on extracting text and metadata features to identify patterns common in spam [6, 7]. However, spammers have proven adept at tweaking their emails to confuse these filters over time.

Received 4 December 2023; accepted 28 May 2024.
Available online 11 February 2025

* Corresponding author.
E-mail address: arfian@umpsa.edu.my (M. A. Ismail).
https://doi.org/10.52866/2788-7421.1236

In recent years, deep learning (DL) has rapidly become state-of-the-art in fields like computer vision [8], speech recognition [9], and natural language processing [10]. Deep neural networks can automatically learn to extract optimal features directly from raw input data through multiple layered transformations [11]. In contrast to earlier machine learning, DL reduces the need for heavily feature engineering pipelines. DL has shown immense success in handling complex, high-dimensional data and continually adapting to tackle variations [8]. These characteristics make DL highly appealing for email spam filtering, which deals with high-dimensional textual data and an adversary that constantly changes tactics [12, 13]. Several studies have confirmed that DL methods can improve upon conventional machine learning techniques for email spam classification [1, 2, 6].

DL has recently gained significant traction for email spam classification, offering potential accuracy improvements over traditional methods [14]. However, the rapid evolution of this field warrants a comprehensive literature review synthesizing the current state of research. Such a review can develop an evidence-based understanding of the strengths and weaknesses of different DL methods for spam detection. Specifically, it can compare the effectiveness of popular approaches like Artificial Neural Network (ANN), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU) and Bidirectional LSTM (Bi-LSTM) while also revealing their limitations and areas needing improvement. A review can further highlight gaps in current knowledge that future research should address. By evaluating findings across pertinent studies, it can identify open questions around model architectures, feature representations, hyperparameter optimization, and other factors influencing performance. Additionally, a review can inform the community's advancement by delineating gaps regarding generalization, concept drift adaptation, and real-world deployment challenges.

There is a dearth of complete and current comprehension of the efficacy, constraints, and prospective avenues for enhancement of these procedures. Although numerous studies have been conducted on the subject, only a limited number have specifically concentrated on employing DL methods for the purpose of email spam categorization. Due to the fast-paced development of this field and the crucial need for precise spam classification, it is imperative to conduct a thorough evaluation that consolidates the current data, identifies any research gaps, and guides the direction of future studies. The contributions of this research is given below:

This research aims to provide a comprehensive overview of the current state of research on the use of DL methods for email spam classification. The review explores the various DL methods used for email spam classification, their effectiveness, and areas for future research, consolidating the findings of pertinent studies to determine the advantages and drawbacks of these methods and offering valuable insights into the obstacles that must be overcome to enhance the precision and efficacy of spam classification.

## 2. Deep learning methods

Detecting email spam poses unique challenges distinct from common cyberattacks exploiting system vulnerabilities. Rather, spam leverages social engineering to manipulate human targets. Effective spam filtering thereby necessitates modeling the linguistic patterns and semantics used in malicious messages. Framing the problem as an instance of text classification, spam detection involves automatically labeling emails as either ham or spam [15]. This motivates the application of DL, which excels at high-dimensional data modeling, like natural language, while requiring minimal feature engineering. Deep neural networks can directly process raw text as input, automatically learning intricate textual patterns for classification [16, 17]. Unlike other machine learning (ML) approaches, deep models can continually update their understanding of language as spammers adapt email verbiage over time. Their representation learning capabilities provide a proficiency in detecting spam amidst constant attempts to disguise malicious content behind informal vocabularies [18]. As spam detection constitutes more than just a technical arms race, DL promises durable gains by revealing foundational inclinations manifesting across spam communications.

DL is an up-and-coming field that uses several nonlinear processing layers to learn features directly from the input, leveraging artificial intelligence (AI) and ML [19]. Email spam detection accuracy may be greatly improved with the help of DL methods. Deng and Yu examined a variety of deep learning techniques, as well as their classification into supervised, unsupervised, and hybrid deep networks depending on the architectures of the networks themselves, as well as applications such as computer vision, language modelling, text processing, multimodal learning, and information retrieval [20, 21]. DL relies on representations of data that include several levels of hierarchy, often in the form of a neural network with more than two layers. Data features from a higher level can be spontaneously integrated into those from a lower level using these methods. Each neuron in a neural network (NN) shares several common characteristics. The number of neurons and their interconnections are in turn determined by the

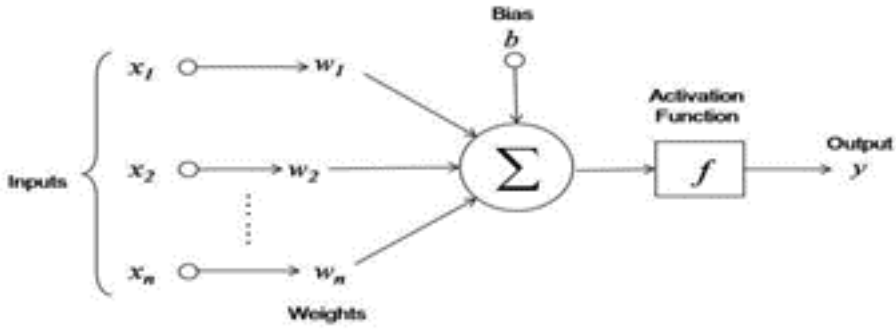


**Fig. 1.** Basic components of ANN architecture.

nature of the application being used [22]. There are many DL methods that are currently and widely used in detecting phishing attacks. These methods, which are chosen because of their high performance and accuracy in detecting email spam, include the ANN, CNN, LSTM, GRU and Bi-LSTM. The explanation of these methods is provided in next sub-sections:

### 2.1. Artificial neural network

The ANN is a way to simulate how signals move through biological NN, like the brain. It does this by having a big network of artificial neurons that are all connected to each other. The ANN has three distinct neuron types: input neurons, hidden neurons, and output neurons [23]. An ANN learns by having its connection weights dynamically adjusted to match the input and output values of the training dataset, with the goal of approximating the mapping function between the input and output values of the network. Starting with the input layer at the very top, the data is processed by the ANN in a hierarchical fashion. In order to determine the activation value associated with the network, the network makes use of a specified activation function [24]. Each neuron's activation and contribution to the overall categorization is decided by the connection weights. In this way, the input to the network, the activation function corresponding to the neurons, the topology of the ANN used, and the connection weights between the various neurons are the primary deciding factors regarding the performance of an ANN. There are two distinct NN architectures in ANN, the feedforward architecture and the feedback architecture, with the former being trained via the recognized backpropagation algorithm. In 2003, a fully connected NN was first used to classify emails using the ANN [25]. The basic components of ANN architecture can be visualized in Fig. 1.

Zhan and his team conducted research on spam classification using the NN method. Their method leverages attributes formed of descriptive aspects of the evasive patterns utilized by spammers, rather than relying on the context or frequency of phrases in the message. Over several months, the researchers compiled a dataset consisting of 2788 legitimate and 1812 spam emails to train and evaluate their model [26]. Additionally, spam email detection models challenges, as it wastes Internet traffic and enables phishing and malware attacks. To address this, a feature selection-based strategy employing the sine-cosine algorithm (SCA) to optimize ANN for spam detection is proposed. Experiments showed the suggested ANN classifier surpassed other methods, achieving precision, accuracy, and sensitivity of 98.64%, 97.92%, and 98.36%, respectively [27]. In this research, an ANN that has been tuned using the Grasshopper Optimization Algorithm (GOA) is used to create a new method for email spam identification. The suggested GOA-ANN method outperforms traditional methods in experiments, achieving 94.25% accuracy in classifying spam. The research shows how bio-inspired algorithms, like GOA, can be used to improve ANN learning for better spam detection [28]. Furthermore, the challenges of constructing efficient ANN structures and tuning parameters for spam detection are examined. A hybrid model combining a genetic algorithm (GA) with an ANN is proposed to optimize spam detection capabilities. Experiments showed the hybrid ANN-GA model performs better in spam detection than conventional ANN methods [29]. Despite taking longer to train, neural networking can classify new patterns and tolerate noisy data.

The research findings indicate that these optimization techniques can improve NN learning and lead to higher spam detection accuracy rates compared to conventional methods. Notably, hybrid models combining NNs with algorithms like GA have demonstrated superior spam detection capabilities,

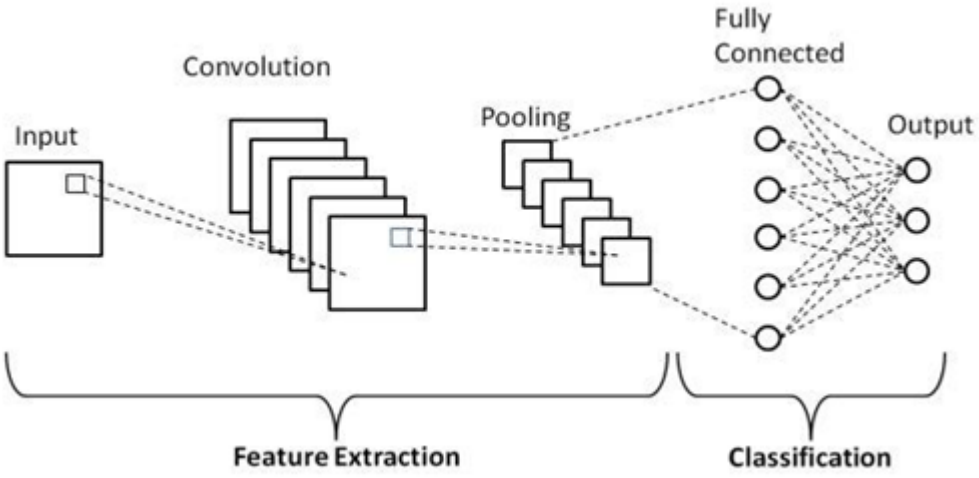


**Fig. 2.** Basic components of CNN architecture.

albeit with longer training times. While constructing efficient NN architectures and tuning parameters remains challenging, the studies suggest that bio-inspired optimization approaches offer promising avenues for optimizing NN models and achieving better spam detection performance, which is crucial for mitigating the negative impacts of spam, such as wasted internet traffic and potential security threats.

### 2.2. Convolutional neural network

As a type of DL method, CNN has recently risen to prominence in the field of computer vision and is gaining attention in other areas, such as defending against email spam. In recent years, CNNs have been a popular topic of study. CNN is useful because it can handle errors well, process information in parallel, and learn on its own. It has been used in the area of email spam filtering with great success. CNNs were described by Albelwi as a type of DL that is based on biology [30]. The network's neurons have weak local connections and a relatively even weight distribution. Multiple trainable layers are stacked atop one another to form a CNN, which is then followed by a supervised classifier and a set of arrays called feature maps that represent the input and output of each layer. Typically, a CNN will have multiple layers, including a convolutional layer, a pooling layer, and a fully connected layer. The use of several layers in CNNs allows for the automatic learning of feature descriptions that are highly discriminative without the use of hand-crafted features [31]. A standard backpropagation NN (BPN) works with isolated hand-crafted image data, while a CNN works specifically on an email to harvest useful, critical features for categorization. The basic components of CNN architecture can be visualized in Fig. 2.

A compared SMS detection using DL classifiers, AI, and CNN have been performed by Gupta [32]. CNN achieved the best accuracy of 99.10% and 98.25% on SMS Spam Collection v.1 and Spam SMS Dataset 2011–12, respectively. Another aspect, the SMS Spam Collection dataset categorizes spam and ham text messages using CNN and LSTM. CNN and LSTM models extracted and categorized vectors. Three CNN layers with dropouts yielded 99.44% accuracy [33]. Moreover, Gupta and his team studied the efficacy of eight different classifiers and compared their results. The results of the classifier evaluation show that the CNN classifier achieves a maximum precision of 99.19% and an Average Recall of 0.9926 and 0.9994, respectively, across the two datasets [30]. As well as a CNN method was developed for SMS spam detection using the Tiago dataset. After preprocessing the text data, including tokenization and stopwords removal, CNN achieved 98.4% accuracy in classifying messages as spam or not spam. The work provides a highly accurate CNN architecture and process for SMS spam detection [34]. In another study, the analyses images using CNN and compares the findings to other ML methods. The CNN-based methodology detects real-world image spam and challenging image spam-like datasets better than earlier methods by using a new feature set mixing raw photos and Canny edges [35].

The research explores various DL methods, particularly CNN for email spam detection. Several studies have demonstrated the superior performance of CNN, achieving high accuracy rates of up to 99.44% on benchmark SMS spam datasets. The findings highlight the efficacy of CNN architectures in extracting

relevant features and accurately classifying SMS spam. Additionally, a CNN-based approach leveraging a combination of raw images and Canny edges outperformed previous methods in detecting real-world image spam and challenging image spam datasets.

### 2.3. Long short-term memory

One popular form of recurrent neural network (RNN) architecture in deep learning is known as LSTM. It was created to solve the issue of disappearing gradients that arise when regular RNNs fail to properly account for temporal dependencies in sequential data. The premise behind LSTM is that data from a long time ago may be useful and should be stored, but that NN have a finite amount of memory [36]. The memory cell is important to LSTM, serving as a unit for storing and updating data. There are three gates in an LSTM model the input gate, the forget gate, and the output gate that control the model's features. Input, forget, and output gates are all included in the memory cell's hardware. New data entering the cell state is regulated by the input gate. The forget gate wipes the cell's state clean of irrelevant data from the past. The next concealed state is determined by the input gate's regulation of information derived from the cell state [37]. Through the use of these gates, an LSTM model can automatically save or delete information from its memory. LSTMs are able to successfully catch and remember essential patterns in sequential data because they can learn to adaptively update the memory cell and manipulate the flow of information. The inclusion of gating mechanisms allows LSTMs to solve the vanishing gradient problem, which is a major benefit of LSTMs. As a result, they are able to learn dependencies with large time lags and can produce reliable predictions based on the full context of the sequence [38]. The basic components of LSTM architecture can be visualized in Fig. 3.

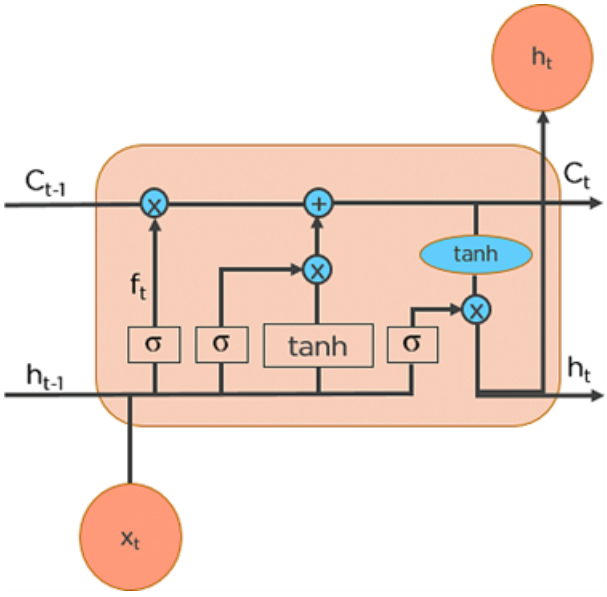


**Fig. 3.** Basic components of LSTM architecture.

Since their introduction, several DL based spam detection algorithms have been proposed. Yang and his team outlined an email classification system called Multi-Modal Architecture with Model Fusion (MMA-MF). The primary focus of this model is to identify spam by processing the email's text and images independently using an LSTM method and a CNN method, respectively. An LSTM model is utilized to determine the likelihood that an email is spam based on its textual content. Meanwhile, a CNN mmethod is used to determine the spam likelihood based on any attached images [39]. In another study, a combined method using an LSTM, Naive Bayes (NB), Logistic Regression (LR), k-NN, random forest (RF), SVM and decision tree (DT) was tested on the UCI SMS spam collection dataset with various embedding techniques (count vectorizer, TF-IDF vectorizer and hashing vectorizer). The highest accuracy of 98.5% was achieved by the LSTM model in this combined architecture [40]. Moreover, a Semantic LSTM (SLSTM) was proposed for spam SMS detection and classification using the SMS Spam Collection dataset and Twitter dataset. The SLSTM incorporates a semantic layer into a LSTM network using Word2Vec word embeddings. Experiments showed the proposed SLSTM technique achieved accuracy results of 99.01% on the SMS Spam Collection dataset and 95.09% on the Twitter dataset [41]. Furthermore, a lightweight GRU (LG-GRU) was employed instead of an LSTM layer for spam classification on the SMS Spam Collection dataset. To improve the semantic understanding of the SMS text inputs, external information from WordNet was incorporated. Compared to LSTM models, the proposed LG-GRU model drastically reduced training time and the number of parameters, while maintaining 99.04% accuracy for spam categorization [42]. Additionally, RNNs are one type of NN that can remember past data but suffer from vanishing and exploding gradient issues. To overcome this drawback, the proposed system leverages the Spambase and Ling Spam datasets to classify spam and ham emails using an LSTM architecture. LSTM keeps track of prior email information and learns to select relevant features while ignoring irrelevant ones for identifying spam. Experiments showed the LSTM method achieves

97.4% accuracy, outperforming other DL methods on these datasets [43]. Moreover, spam emails are used for propaganda, advertising, and phishing, which can financially and morally harm internet users as well as disrupt internet traffic. To address this issue, detected spam emails in a Turkish dataset with 100% accuracy using the Keras library and LSTM method. The results demonstrated that an LSTM based method was highly effective for spam detection in Turkish emails [44]. Furthermore, spam emails cause issues like network disruption and cybercrime. A sentiment analysis-friendly spam mail detection method was proposed using Word Embedding techniques including Bag of Words, Hashing, and an LSTM method. Experiments on a dataset of 5,572 messages showed the proposed technique achieved 93–98% in precision, recall, F1-score, and accuracy [45].

The development of ensemble methods that have the potential to integrate the advantages of LSTM with traditional ML methods could be the focus of future research areas. This approach could potentially further improve spam detection accuracy across various data types. Additionally, exploring transfer learning approaches by leveraging pre-trained DL methods on large datasets could reduce training time and data requirements for spam detection tasks. For low-resource languages or domains with limited labeled data, developing more robust and efficient DL methods is crucial. Incorporating advanced natural language processing techniques, such as attention mechanisms and transformer models, into DL architectures could enhance the understanding of textual content and context, leading to better spam detection performance.

### 2.4. Gated recurrent unit

GRU is a type of RNN that is well-suited for sequence modeling tasks. The GRU model introduced by Cho also addresses the vanishing gradient problem prevalent in RNN [46]. The GRU architecture is similar to LSTM in that it contains gating units to control the flow of information. However, GRU lacks an output gate and uses fewer parameters than LSTM, resulting in faster computation times during training [47]. Specifically, the GRU architecture consists of a reset gate and an update gate. The reset gate determines how much past information to forget, while the update gate decides how much past information to pass along to the future [48]. The current memory content is stored in a hidden state vector, which is a linear combination of the previous hidden state and the current input modulated by the update gate. The basic components of GRU architecture can be visualized in Fig. 4.

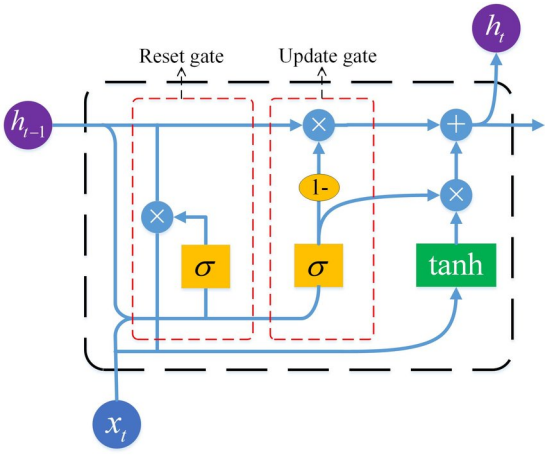


**Fig. 4.** Basic components of GRU architecture.

Email spam detection poses a sequence modeling problem well-suited for GRU. A GRU-based architecture for spam detection would process the email text sequentially, encoding each word into a hidden state vector. The gating units in the GRU regulate the flow of information, learning to identify key words and phrases that serve as indicators of spam or legitimate emails [49]. Additionally, as the GRU progresses through the email text, its hidden state captures relevant context and sequentially whether the message is likely to be spam or not. The ability of GRUs to selectively propagate relevant information while processing variable length sequences makes them a promising approach for modeling email text for spam detection [50]. Moreover, a new DL approach uses CNN and RNN to analyze email communication by classifying message components into zones. The method leverages GRU-CRF to segment emails into zones like header, quotation, greeting, and body. Experiments show the technique achieves 98% accuracy on zone prediction, outperforming traditional methods, with improved adaptability and resilience [51]. Furthermore, a lightweight GRU (LG-GRU) was employed instead of an LSTM layer for spam classification on the SMS Spam Collection dataset. To improve the semantic understanding of the SMS text inputs, external information from WordNet was incorporated. Compared to LSTM methods, the proposed LG-GRU model drastically reduced training time and the number of parameters, while maintaining 99.04% accuracy for spam categorization [42].

GRU presents a promising approach for email spam detection, as it is a sequence modeling problem well-suited for this type of recurrent neural network architecture. A GRU-based model would process email text sequentially, encoding each word into a hidden state vector while using gating units to

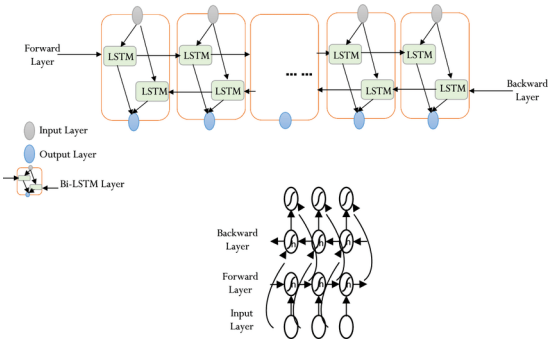


**Fig. 5.** Basic components of Bi-LSTM architecture.

regulate the flow of information. This allows the GRU to learn and identify key words and phrases indicative of spam or legitimate emails. As the GRU progresses through the email text, its hidden state captures relevant context and sequentially determines whether the message is likely spam or not. The ability of GRUs to selectively propagate relevant information while processing variable-length sequences makes them well-suited for modeling email text for spam detection.

### 2.5. Bidirectional long short-term memory

Bidirectional LSTM (Bi-LSTM) is an extension of traditional LSTM architectures for sequence modeling tasks. In a Bi-LSTM, two LSTMs process the input sequence in forward and backward directions, allowing the model to learn both past and future context. The two directional outputs are concatenated to form the final output at each time step [52]. The Bi-LSTM model has the ability to retain and recall lengthier sequences of data, in addition to its capability to generate predictions for textual data. This approach enhances its data storage capacity by enabling bidirectional processing [53]. The Bi-LSTM model is capable of preserving the contextual information of the given data by predicting the preceding or next word in a sentence. Bi-LSTM gives the best results possible for many sequence modelling tasks where the full contextual information is important [54]. The basic components of Bi-LSTM architecture can be visualized in Fig. 5.

The task of email spam detection involves the construction of models that capture the contextual information of words inside an email, enabling the determination of whether the email's content may be classified as spam or not. The Bi-LSTM model is very suitable for this particular task because of its ability to effectively capture both semantic and syntactic links between words. This is achieved by processing the email content in both forward and backward orientations [55]. Additionally, a new DL model for email spam detection using sentiment analysis of email text, combining WordEmbeddings, CNN, and Bi-LSTM networks to analyze textual and sequential properties. Evaluated on two spam datasets, the method achieves improved accuracy of 98–99% and outperforms popular classifiers and state-of-the-art methods, proving its superiority for spam detection [56]. Moreover, spam emails are becoming more common and troublesome as email usage grows, there is a need for effective methods to detect spam. A recent study compared different ML and DL models, such as NB, RF, ANN, SVM, LSTM, and Bi-LSTM, for the task of identifying spam emails. The study found that Bi-LSTM had the best accuracy of 98.57% for spam prediction [57]. Furthermore, spam text messages steal information from users and hurt them, but the methods available for finding them aren't good enough. The vectorization-based feature engineering and Bi-LSTM networks can be used together to make an effective predictor that can find spam SMS. Experiments showed that the method is more accurate than other methods in terms of precision, recall, and F1 measures [58].

Bi-LSTM methods for spam detection could explore hybrid architectures that combine Bi-LSTMs with other DL components to further enhance contextual understanding and spam detection performance. Expanding the datasets used, including multilingual and cross-domain corpora, could assess the methods' robustness and generalization abilities. Incorporating external knowledge, domain-specific features, and semantic information could lead to more comprehensive and effective Bi-LSTM-based spam detection systems. Developing explainable and interpretable Bi-LSTM methods would facilitate trust and understanding of the decision-making process. Adapting Bi-LSTM methods to detect emerging spam threats, such as those involving multimedia content and new evasion techniques, would ensure the methods remain effective in the face of changing spam patterns.

## 3. Comparative analysis of deep learning methods

Numerous considerations must be made in order to select the most appropriate DL approach for email spam classification. Processing speed, classifier accuracy, data amount and complexity, and the interpretability of the DL method's output model are typically among the several parameters that impact the method's performance and accuracy. Table 1 provides a comparative analysis of the DL methods.

Current understanding of the effectiveness, limitations, and potential advancements of DL based email spam categorization methodologies

**Table 1.** Comparative analysis of DL methods.

| Method | Advantages | Disadvantages |
|---|---|---|
| Artificial Neural Network | ANN can learn from data to generalize to new situations [59]. | ANN require substantial training data and computing resources [24]. |
| | Handle nonlinear and complex problems [25]. | Prone to overfitting [60]. |
| | Approximate complex functions given sufficient data [61]. | Lack interpretability into predictions [62]. |
| | Enable parallel and distributed processing [63]. | Sensitive to choose of hyperparameters [64]. |
| | Adapt to changing environments [65]. | Can get trapped in suboptimal solutions [66]. |
| Convolutional Neural Network | CNN provide very high accuracy for image recognition tasks [67] | CNN does not encode the position and orientation of objects [68]. |
| | Automatically extract important features [69]. | Lack full spatial invariance [70]. |
| | Weight sharing reduces overfitting [71]. | Require lots of data and computing resources [72]. |
| | Invariant to translations, rotations and scaling [73]. | Hard to design optimal architecture [74]. |
| | Can combine with RNN or LSTM for multimodal tasks [75]. | Can suffer from exploding/vanishing gradients [76]. |
| Long Short-Term Memory Network | LSTM can learn long-term sequential dependencies [77]. | LSTM has many parameters requiring substantial data or compute [78]. |
| | Handle variable-length sequence data [79]. | Suffer from exploding gradients [80]. |
| | Avoid vanishing gradients with gates and cells [81]. | Lack interpretability [82]. |
| | Model complex sequence relationships [83]. | Sensitive to hyperparameters [84]. |
| | Wide applicability (NLP, speech, etc) [85]. | Can overfit or underfit [86]. |
| Gated Recurrent Unit | GRU is a simplified version of LSTM [87]. | GRU provide lower accuracy than LSTM on large datasets [88]. |
| | Fewer parameters and faster execution [89]. | Still susceptible to exploding gradients |
| | Can handle variable-length inputs and outputs [90]. | Lack interpretability [91]. |
| | Handle long sequences while avoiding vanishing gradients [92]. | Sensitive to hyperparameters [93]. |
| | Model complex sequential relationships [94]. | Overfitting or underfitting issues [95]. |
| Bidirectional-LSTM | Bi-LSTM can capture both forward and backward sequence context [96]. | Bi-LSTM has double the parameters of LSTM [97]. |
| | Improves sequence modeling performance [98]. | Requires more data and computing [99]. |
| | Handle variable-length sequences [100]. | Suffers from exploding gradients [101]. |
| | Avoid vanishing gradients with gates or cells [102]. | Lack interpretability [103]. |
| | Model complex sequence relationships [104]. | Sensitive to hyperparameters [105]. |

remains incomplete and outdated. Though numerous studies have explored email spam filtering broadly, few have specifically focused their investigation on applying DL methods to the problem of email spam classification. Considering the rapid pace of advancement in this field and the critical need for accurate identification of spam emails, conducting an exhaustive review that synthesizes present knowledge, illuminates gaps in the literature, and directs future research is imperative. By thoroughly evaluating the existing body of work concentrated explicitly on utilizing DL for email spam categorization, a comprehensive grasp can be gained of the efficacy of these approaches, constraints still to be addressed, and promising directions for refinement. Consolidating current findings, pinpointing outstanding questions, and mapping future directions will prove vital for continued progress as the improvement continues evolving rapidly amidst a pressing need for precise spam classify capabilities.

## 4. Anti-spam strategies and need for spam classification

### *4.1. Anti-spam strategies*

Anti-spam strategies fall into three categories - prevention, detection, and demotion - to combat unwanted messages and content. Fig. 6 provide the anti-spam strategies.

- Prevention Based: These strategies aim to stop spammers from creating or sending spam in the first place [106]. For example, CAPTCHAs are tests that require users to prove that they are human and not automated bots. Account Fees are

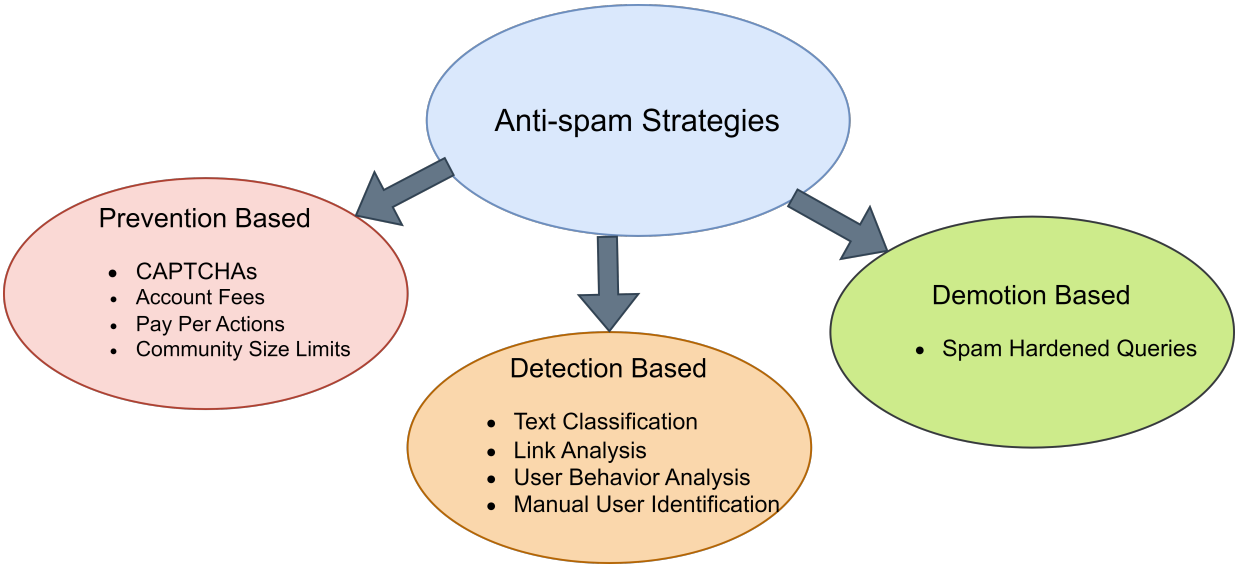


**Fig. 6.** Anti-spam strategies.

charges that users have to pay to create or use an account on a platform. Pay Per Actions are fees that users have to pay for each action they perform on a platform, such as posting, commenting, or liking. Community Size Limits are restrictions that limit the number of users or connections that a user can have on a platform.

- Detection Based: These strategies aim to identify and flag spam messages or content after they are created or sent [107]. For example, Text Classification is a technique that uses ML or natural language processing to analyze the text of a message or content and determine if it is spam or not. Link Analysis is a technique that examines the links or URLs in a message or content and checks if they are malicious or fraudulent. User Behavior Analysis is a technique that monitors the actions and interactions of a user on a platform and detects any abnormal or suspicious patterns. Manual User Identification is a technique that requires users to verify their identity or authenticity through human moderators or reviewers.
- Demotion Based: These strategies aim to reduce the visibility or impact of spam messages or content on the internet [108]. For example, Spam Hardened Queries are queries that are designed to filter out or rank lower spam results from a search engine.

### *4.2. Need for spam classification*

There is a lot of spam on the internet, which is bad for viewers and makes things harder for businesses around the world. The widespread use of spam has many bad effects, such as

- Search engines losing their usefulness, fewer people visiting real sites, and less money for those sites.
- Bringing unwanted web traffic to websites and giving illegal businesses free advertising by spreading spam.
- The destruction of user trust and loyalty towards search providers is due to the ease with which users can switch between them.
- Facilitating the dissemination of malware, explicit material, and phishing schemes by acting as a proxy.
- Requiring accurate labeling of material in order to effectively identify and remove spam in order to enhance relevance.

## 5. Challenges

Several key challenges remain in applying DL to email spam classification.

Imbalanced datasets with far more legitimate emails than spam continue to bias models towards false positives. Techniques like oversampling minority classes during training are actively being researched. The dynamic evolution of spam tactics reduces method generalization to new attacks. Ensuring robustness through adversarial training approaches is an open area. Potential adversarial manipulations specifically aimed at evading deep learning models pose reliability threats. Detection of adversarial samples and training on adversarial

datasets helps harden methods. The black-box nature of deep nets hampers interpretability in their decision-making process. Explainable AI methods to increase transparency and trust around model behaviors are still maturing. The significant computational resources required for large-scale DL training remains challenging for smaller organizations. Efficiency optimizations around neural architectures and hardware acceleration are lowering costs. Generalizability across diverse email platforms and user populations is critical for broad deployment. Multi-domain learning and personalization techniques are active research directions. The privacy implications of content analysis and integration with existing infrastructure having varied platforms and minimally disrupted user experiences bring deployment and adoption hurdles. Limited labeled data for training deep nets well continues to be an industry-wide bottleneck. Data augmentation, transfer learning, and semi-supervised techniques are advancing to multiply limited labeled data. Meeting the real-time latency constraints of live email traffic with deep methods poses throughput challenges. Quantization, pruning, and efficient model distillation methods are improving inferencing speed.

## 6. Conclusions

In recent years, DL techniques have emerged as powerful approaches for performing highly accurate email spam classification. This paper reviewed five prevalent DL classification techniques for their application in email spam detection. The methods analyzed include ANN, CNN, LSTM, GRU and Bi-LSTM networks. For each approach, the discussion covers the underlying mechanisms, strengths, and limitations. This comprehensive review has highlighted several frontiers and research gaps pertaining to the application of DL for email spam classification. The limitations centered on model complexity, feature representation, class imbalance, and lack of ensemble modeling provide avenues for further investigation. Nevertheless, DL methods have proven highly promising in their capability to understand complex semantic relationships and automatically extract informative feature representations from raw email data. As email spamming techniques continue to evolve, DL presents a promising set of techniques to maintain robust classify capabilities. With continued research addressing current limitations, hybrid neural networks are likely to proliferate further as the premier approach to classifying email spam.

## Funding

This study was supported by Fundamental Research Grant (FRGS) with FRGS/1/2022/ICT02/UMP/02/2 (RDU220134) from the Ministry of Higher Education Malaysia.

## References

1. K. Thakur, M. L. Ali, M. A. Obaidat, and A. Kamruzzaman, “A systematic review on deep-learning-based phishing email detection,” *Electronics*, vol. 12, no. 21, p. 4545, 2023.
2. A. Karim, S. Azam, B. Shanmugam, K. Kannoorpatti, and M. Alazab, “A comprehensive survey for intelligent spam email detection,” *IEEE Access*, vol. 7, pp. 168261–168295, 2019.
3. R. Mansoor, N. D. Jayasinghe, and M. M. A. Muslam, “A comprehensive review on email spam classification using machine learning algorithms,” in *2021 International Conference on Information Networking (ICOIN)*, pp. 327–332, IEEE, 2021.
4. H. Kumar, P. J. Soh, and M. A. Ismail, “Big data streaming platforms: A review,” *Iraqi Journal for Computer Science and Mathematics*, vol. 3, no. 2, pp. 95–100, 2022.
5. F. Jáñez-Martino, R. Alaiz-Rodríguez, V. González-Castro, E. Fidalgo, and E. Alegre, “A review of spam email detection: analysis of spammer strategies and the dataset shift problem,” *Artificial Intelligence Review*, vol. 56, no. 2, pp. 1145–1173, 2023.
6. E. G. Dada, J. S. Bassi, H. Chiroma, A. O. Adetunmbi, O. E. Ajibuwa, *et al.*, “Machine learning for email spam filtering: review, approaches and open research problems,” *Heliyon*, vol. 5, no. 6, 2019.
7. N. S. Nordin and M. A. Ismail, “A hybridization of butterfly optimization algorithm and harmony search for fuzzy modelling in phishing attack detection,” *Neural Computing and Applications*, vol. 35, no. 7, pp. 5501–5512, 2023.
8. J. U. M. Akbar, S. F. Kamarulzaman, A. J. M. Muzahid, M. A. Rahman, and M. Uddin, “A comprehensive review on deep learning assisted computer vision techniques for smart greenhouse agriculture,” *IEEE Access*, 2024.
9. I. H. Sarker, “Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions,” *SN Computer Science*, vol. 2, no. 6, p. 420, 2021.
10. M. Z. Alom, T. M. Taha, C. Yakopcic, S. Westberg, P. Sidike, M. S. Nasrin, M. Hasan, B. C. Van Essen, A. A. Awwal, and V. K. Asari, “A state-of-the-art survey on deep learning theory and architectures,” *Electronics*, vol. 8, no. 3, p. 292, 2019.
11. G. Kocher and G. Kumar, “Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges,” *Soft Computing*, vol. 25, no. 15, pp. 9731–9763, 2021.
12. Z. Alshingiti, R. Alaqel, J. Al-Muhtadi, Q. E. U. Haq, K. Saleem, and M. H. Faheem, “A deep learning-based phishing detection system using cnn, lstm, and lstm-cnn,” *Electronics*, vol. 12, no. 1, p. 232, 2023.
13. N. N. M. Azam, M. A. Ismail, M. S. Mohamad, A. O. Ibrahim, and S. Jeba, “Classification of covid-19 symptoms using multilayer perceptron,” *Iraqi Journal For Computer Science and Mathematics*, vol. 4, no. 4, pp. 100–110, 2023.

14. Q. Yaseen *et al.*, "Spam email detection using deep learning techniques," *Procedia Computer Science*, vol. 184, pp. 853–858, 2021.
15. N. Hussain, H. Turab Mirza, G. Rasool, I. Hussain, and M. Kaleem, "Spam review detection techniques: A systematic literature review," *Applied Sciences*, vol. 9, no. 5, p. 987, 2019.
16. S. Srinivasan, V. Ravi, M. Alazab, S. Ketha, A. M. Al-Zoubi, and S. Kotti Padannayil, "Spam emails detection based on distributed word embedding with deep learning," *Machine intelligence and big data analytics for cybersecurity applications*, pp. 161–189, 2021.
17. N. S. Nordin, M. A. Ismail, T. Sutikno, S. Kasim, R. Hassan, Z. Zakaria, and M. S. Mohamad, "A comparative analysis of metaheuristic algorithms in fuzzy modelling for phishing attack detection," *Indones. J. Electr. Eng. Comput. Sci*, vol. 23, no. 2, pp. 1146–1158, 2021.
18. U. A. Butt, R. Amin, H. Aldabbas, S. Mohan, B. Alouffi, and A. Ahmadian, "Cloud-based email phishing attack using machine and deep learning algorithm," *Complex & Intelligent Systems*, vol. 9, no. 3, pp. 3043–3070, 2023.
19. J. U. M. Akbar, S. F. Kamarulzaman, and E. H. Tusher, "Plant stem disease detection using machine learning approaches," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1–8, IEEE, 2023.
20. S. Dong, P. Wang, and K. Abbas, "A survey on deep learning and its applications," *Computer Science Review*, vol. 40, p. 100379, 2021.
21. L. Santos, F. N. Santos, P. M. Oliveira, and P. Shinde, "Deep learning applications in agriculture: A short review," in *Robot 2019: Fourth Iberian Robotics Conference: Advances in Robotics, Volume 1*, pp. 139–151, Springer, 2020.
22. Y. Guo, Y. Liu, A. Oerlemans, S. Lao, S. Wu, and M. S. Lew, "Deep learning for visual understanding: A review," *Neurocomputing*, vol. 187, pp. 27–48, 2016.
23. M. Chen, U. Challita, W. Saad, C. Yin, and M. Debbah, "Artificial neural networks-based machine learning for wireless networks: A tutorial," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3039–3071, 2019.
24. O. I. Abiodun, A. Jantan, A. E. Omolara, K. V. Dada, A. M. Umar, O. U. Linus, H. Arshad, A. A. Kazaure, U. Gana, and M. U. Kiru, "Comprehensive review of artificial neural network applications to pattern recognition," *IEEE access*, vol. 7, pp. 158820–158846, 2019.
25. P. G. Asteris and V. G. Mokos, "Concrete compressive strength using artificial neural networks," *Neural Computing and Applications*, vol. 32, no. 15, pp. 11807–11826, 2020.
26. C. Zhan, F. Zhang, and M. Zheng, "Design and implementation of an optimization system of span filter rule based on neural network," in *2007 International Conference on Communications, Circuits and Systems*, pp. 882–886, IEEE, 2007.
27. R. Talaei Pashiri, Y. Rostami, and M. Mahrami, "Spam detection through feature selection using artificial neural network and sine–cosine algorithm," *Mathematical Sciences*, vol. 14, pp. 193–199, 2020.
28. S. A. Ghaleb, M. Mohamad, E. F. H. S. Abdullah, and W. A. Ghanem, "Spam classification based on supervised learning using grasshopper optimization algorithm and artificial neural network," in *Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers 2*, pp. 420–434, Springer, 2021.
29. A. Arram, H. Mousa, and A. Zainal, "Spam detection using hybrid artificial neural network and genetic algorithm," in *2013 13th International Conference on Intellient Systems Design and Applications*, pp. 336–340, IEEE, 2013.
30. J. Gu, Z. Wang, J. Kuen, L. Ma, A. Shahroudy, B. Shuai, T. Liu, X. Wang, G. Wang, J. Cai, *et al.*, "Recent advances in convolutional neural networks," *Pattern recognition*, vol. 77, pp. 354–377, 2018.
31. Z. Li, F. Liu, W. Yang, S. Peng, and J. Zhou, "A survey of convolutional neural networks: analysis, applications, and prospects," *IEEE transactions on neural networks and learning systems*, 2021.
32. V. Gupta, A. Mehta, A. Goel, U. Dixit, and A. C. Pandey, "Spam detection using ensemble learning," in *Harmony Search and Nature Inspired Optimization Algorithms: Theory and Applications, ICHSA 2018*, pp. 661–668, Springer, 2019.
33. P. K. Roy, J. P. Singh, and S. Banerjee, "Deep learning to filter sms spam," *Future Generation Computer Systems*, vol. 102, pp. 524–533, 2020.
34. M. Popovac, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, "Convolutional neural network based sms spam detection," in *2018 26th Telecommunications forum (TELFOR)*, pp. 1–4, IEEE, 2018.
35. T. Sharmin, F. Di Troia, K. Potika, and M. Stamp, "Convolutional neural networks for image spam detection," *Information Security Journal: A Global Perspective*, vol. 29, no. 3, pp. 103–117, 2020.
36. G. Van Houdt, C. Mosquera, and G. Nápoles, "A review on the long short-term memory model," *Artificial Intelligence Review*, vol. 53, pp. 5929–5955, 2020.
37. T. Muralidharan and N. Nissim, "Improving malicious email detection through novel designated deep-learning architectures utilizing entire email," *Neural Networks*, vol. 157, pp. 257–279, 2023.
38. Q. Li, M. Cheng, J. Wang, and B. Sun, "Lstm based phishing detection for big email data," *IEEE transactions on big data*, vol. 8, no. 1, pp. 278–288, 2020.
39. H. Yang, Q. Liu, S. Zhou, and Y. Luo, "A spam filtering method based on multi-modal fusion," *Applied Sciences*, vol. 9, no. 6, p. 1152, 2019.
40. S. Gadde, A. Lakshmanarao, and S. Satyanarayana, "Sms spam detection using machine learning and deep learning techniques," in *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, vol. 1, pp. 358–362, IEEE, 2021.
41. G. Jain, M. Sharma, and B. Agarwal, "Optimizing semantic lstm for spam detection," *International Journal of Information Technology*, vol. 11, pp. 239–250, 2019.
42. F. Wei and T. Nguyen, "A lightweight deep neural model for sms spam detection," in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–6, IEEE, 2020.
43. V. S. Vinitha, D. K. Renuka, and L. A. Kumar, "Long short-term memory networks for email spam classification," in *2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS)*, pp. 176–180, IEEE, 2023.
44. E. E. Eryılmaz, D. Ö. Şahin, and E. Kılıç, "Filtering turkish spam using lstm from deep learning techniques," in *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1–6, IEEE, 2020.
45. S. Thanarattananakin, S. Bulao, B. Visitsilp, and M. Maliyaem, "Spam detection using word embedding-based lstm," in *2022 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications*

*Engineering (ECTI DAMT & NCON)*, pp. 227–231, IEEE, 2022.
46. K. Cho, B. Van Merriënboer, D. Bahdanau, and Y. Bengio, "On the properties of neural machine translation: Encoder-decoder approaches," *arXiv preprint arXiv:1409.1259*, 2014.
47. R. Fu, Z. Zhang, and L. Li, "Using lstm and gru neural network methods for traffic flow prediction," in *2016 31st Youth academic annual conference of Chinese association of automation (YAC)*, pp. 324–328, IEEE, 2016.
48. R. Dey and F. M. Salem, "Gate-variants of gated recurrent unit (gru) neural networks," in *2017 IEEE 60th international midwest symposium on circuits and systems (MWSCAS)*, pp. 1597–1600, IEEE, 2017.
49. K. A. Al-Thelaya, T. S. Al-Nethary, and E. Y. Ramadan, "Social networks spam detection using graph-based features analysis and sequence of interactions between users," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pp. 206–211, IEEE, 2020.
50. A. A. Abdullahi and M. Kaya, "A deep learning based method to detect email and sms spams," in *2021 International Conference on Decision Aid Sciences and Application (DASA)*, pp. 430–435, IEEE, 2021.
51. T. Repke and R. Krestel, "Bringing back structure to free text email conversations with recurrent neural networks," in *Advances in Information Retrieval: 40th European Conference on IR Research, ECIR 2018, Grenoble, France, March 26-29, 2018, Proceedings 40*, pp. 114–126, Springer, 2018.
52. F. Shahid, A. Zameer, and M. Muneeb, "Predictions for covid-19 with deep learning models of lstm, gru and bi-lstm," *Chaos, Solitons & Fractals*, vol. 140, p. 110212, 2020.
53. T. Le, M. T. Vo, B. Vo, E. Hwang, S. Rho, and S. W. Baik, "Improving electric energy consumption prediction using cnn and bi-lstm," *Applied Sciences*, vol. 9, no. 20, p. 4237, 2019.
54. Q. Sun, M. V. Jankovic, L. Bally, and S. G. Mougiakakou, "Predicting blood glucose with an lstm and bi-lstm based deep neural network," in *2018 14th symposium on neural networks and applications (NEUREL)*, pp. 1–5, IEEE, 2018.
55. S. M. Zaman, M. M. Hasan, R. I. Sakline, D. Das, and M. A. Alam, "A comparative analysis of optimizers in recurrent neural networks for text classification," in *2021 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, pp. 1–6, IEEE, 2021.
56. S. E. Rahman and S. Ullah, "Email spam detection using bidirectional long short term memory with convolutional neural network," in *2020 IEEE Region 10 Symposium (TENSYMP)*, pp. 1307–1311, IEEE, 2020.
57. C. M. Shaik, N. M. Penumaka, S. K. Abbireddy, V. Kumar, and S. Aravinth, "Bi-lstm and conventional classifiers for email spam filtering," in *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, pp. 1350–1355, IEEE, 2023.
58. A. L. Rosewelt, N. D. Raju, and S. Ganapathy, "An effective spam message detection model using feature engineering and bi-lstm," in *2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, pp. 1–6, IEEE, 2022.
59. F.-L. Fan, J. Xiong, M. Li, and G. Wang, "On interpretability of artificial neural networks: A survey," *IEEE Transactions on Radiation and Plasma Medical Sciences*, vol. 5, no. 6, pp. 741–760, 2021.
60. G. M. Van de Ven, H. T. Siegelmann, and A. S. Tolias, "Brain-inspired replay for continual learning with artificial neural networks," *Nature communications*, vol. 11, no. 1, p. 4069, 2020.
61. Y. Chen, L. Song, Y. Liu, L. Yang, and D. Li, "A review of the artificial neural network models for water quality prediction," *Applied Sciences*, vol. 10, no. 17, p. 5776, 2020.
62. J. Tang, F. Yuan, X. Shen, Z. Wang, M. Rao, Y. He, Y. Sun, X. Li, W. Zhang, Y. Li, *et al.*, "Bridging biological and artificial neural networks with emerging neuromorphic devices: fundamentals, progress, and challenges," *Advanced Materials*, vol. 31, no. 49, p. 1902761, 2019.
63. J. Runge and R. Zmeureanu, "Forecasting energy use in buildings using artificial neural networks: A review," *Energies*, vol. 12, no. 17, p. 3254, 2019.
64. K. Ostad-Ali-Askari and M. Shayan, "Subsurface drain spacing in the unsteady conditions by hydrus-3d and artificial neural networks," *Arabian Journal of Geosciences*, vol. 14, pp. 1–14, 2021.
65. E. Haghighat and R. Juanes, "Sciann: A keras/tensorflow wrapper for scientific computations and physics-informed deep learning using artificial neural networks," *Computer Methods in Applied Mechanics and Engineering*, vol. 373, p. 113552, 2021.
66. C. G. Villegas-Mier, J. Rodriguez-Resendiz, J. M. Álvarez-Alvarado, H. Rodriguez-Resendiz, A. M. Herrera-Navarro, and O. Rodríguez-Abreo, "Artificial neural networks in mppt algorithms for optimization of photovoltaic power systems: A review," *Micromachines*, vol. 12, no. 10, p. 1260, 2021.
67. L. Chen, S. Li, Q. Bai, J. Yang, S. Jiang, and Y. Miao, "Review of image classification algorithms based on convolutional neural networks," *Remote Sensing*, vol. 13, no. 22, p. 4712, 2021.
68. S. Kiranyaz, O. Avci, O. Abdeljaber, T. Ince, M. Gabbouj, and D. J. Inman, "1d convolutional neural networks and applications: A survey," *Mechanical systems and signal processing*, vol. 151, p. 107398, 2021.
69. M. Krichen, "Convolutional neural networks: A survey," *Computers*, vol. 12, no. 8, p. 151, 2023.
70. O. A. Saltykova *et al.*, "Cnn-ps: Electroencephalogram classification of brain states using hybrid machine-deep learning approach," *Iraqi Journal For Computer Science and Mathematics*, vol. 4, no. 4, pp. 63–75, 2023.
71. N. Ketkar, J. Moolayil, N. Ketkar, and J. Moolayil, "Convolutional neural networks," *Deep Learning with Python: Learn Best Practices of Deep Learning Models with PyTorch*, pp. 197–242, 2021.
72. D.-X. Zhou, "Theory of deep convolutional neural networks: Downsampling," *Neural Networks*, vol. 124, pp. 319–327, 2020.
73. M. Sarıgül, B. M. Ozyildirim, and M. Avci, "Differential convolutional neural network," *Neural Networks*, vol. 116, pp. 279–287, 2019.
74. S. R. Dubey, S. Chakraborty, S. K. Roy, S. Mukherjee, S. K. Singh, and B. B. Chaudhuri, "diffgrad: an optimization method for convolutional neural networks," *IEEE transactions on neural networks and learning systems*, vol. 31, no. 11, pp. 4500–4511, 2019.
75. A. Dhillon and G. K. Verma, "Convolutional neural network: a review of models, methodologies and applications to object detection," *Progress in Artificial Intelligence*, vol. 9, no. 2, pp. 85–112, 2020.
76. T. Kattenborn, J. Leitloff, F. Schiefer, and S. Hinz, "Review on convolutional neural networks (cnn) in vegetation remote sensing," *ISPRS journal of photogrammetry and remote sensing*, vol. 173, pp. 24–49, 2021.
77. B. Lindemann, T. Müller, H. Vietz, N. Jazdi, and M. Weyrich, "A survey on long short-term memory networks for time series prediction," *Procedia CIRP*, vol. 99, pp. 650–655, 2021.

78. W. Cai, W. Zhang, X. Hu, and Y. Liu, "A hybrid information model based on long short-term memory network for tool condition monitoring," *Journal of Intelligent Manufacturing*, vol. 31, pp. 1497–1510, 2020.
79. S. Ghimire, Z. M. Yaseen, A. A. Farooque, R. C. Deo, J. Zhang, and X. Tao, "Streamflow prediction using an integrated methodology based on convolutional neural network and long short-term memory networks," *Scientific Reports*, vol. 11, no. 1, p. 17497, 2021.
80. L. Han, H. Jing, R. Zhang, and Z. Gao, "Wind power forecast based on improved long short term memory network," *Energy*, vol. 189, p. 116300, 2019.
81. W. Li, N. Sengupta, P. Dechent, D. Howey, A. Annaswamy, and D. U. Sauer, "Online capacity estimation of lithium-ion batteries with deep long short-term memory networks," *Journal of power sources*, vol. 482, p. 228863, 2021.
82. S. Fan, N. Xiao, and S. Dong, "A novel model to predict significant wave height based on long short-term memory network," *Ocean Engineering*, vol. 205, p. 107298, 2020.
83. H. Fan, M. Jiang, L. Xu, H. Zhu, J. Cheng, and J. Jiang, "Comparison of long short term memory networks and the hydrological model in runoff simulation," *Water*, vol. 12, no. 1, p. 175, 2020.
84. P. Park, P. D. Marco, H. Shin, and J. Bang, "Fault detection and diagnosis using combined autoencoder and long short-term memory network," *Sensors*, vol. 19, no. 21, p. 4612, 2019.
85. J. Ma, Z. Li, J. C. Cheng, Y. Ding, C. Lin, and Z. Xu, "Air quality prediction at new stations using spatially transferred bi-directional long short-term memory network," *Science of The Total Environment*, vol. 705, p. 135771, 2020.
86. Y. Huang, X. Dai, Q. Wang, and D. Zhou, "A hybrid model for carbon price forecasting using garch and long short-term memory network," *Applied Energy*, vol. 285, p. 116485, 2021.
87. A. Dutta, S. Kumar, and M. Basu, "A gated recurrent unit approach to bitcoin price prediction," *Journal of risk and financial management*, vol. 13, no. 2, p. 23, 2020.
88. Z. Niu, Z. Yu, W. Tang, Q. Wu, and M. Reformat, "Wind power forecasting using attention-based gated recurrent unit network," *Energy*, vol. 196, p. 117081, 2020.
89. Y.-g. Zhang, J. Tang, Z.-y. He, J. Tan, and C. Li, "A novel displacement prediction method using gated recurrent unit model with time series analysis in the erdaohe landslide," *Natural Hazards*, vol. 105, pp. 783–813, 2021.
90. Q. Ni, J. Ji, and K. Feng, "Data-driven prognostic scheme for bearings based on a novel health indicator and gated recurrent unit network," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1301–1311, 2022.
91. Z. Huang, F. Yang, F. Xu, X. Song, and K.-L. Tsui, "Convolutional gated recurrent unit–recurrent neural network for state-of-charge estimation of lithium-ion batteries," *Ieee Access*, vol. 7, pp. 93139–93149, 2019.
92. Y.-W. Lu, C.-Y. Hsu, and K.-C. Huang, "An autoencoder gated recurrent unit for remaining useful life prediction," *Processes*, vol. 8, no. 9, p. 1155, 2020.
93. Z. Que, X. Jin, and Z. Xu, "Remaining useful life prediction for bearings based on a gated recurrent unit," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–11, 2021.
94. J. Zhang, Y. Jiang, S. Wu, X. Li, H. Luo, and S. Yin, "Prediction of remaining useful life based on bidirectional gated recurrent unit with temporal self-attention mechanism," *Reliability Engineering & System Safety*, vol. 221, p. 108297, 2022.
95. Z. Chen, H. Zhao, Y. Zhang, S. Shen, J. Shen, and Y. Liu, "State of health estimation for lithium-ion batteries based on temperature prediction and gated recurrent unit neural network," *Journal of Power Sources*, vol. 521, p. 230892, 2022.
96. Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, "A bidirectional lstm deep learning approach for intrusion detection," *Expert Systems with Applications*, vol. 185, p. 115524, 2021.
97. K. U. Jaseena and B. C. Kovoor, "Decomposition-based hybrid wind speed forecasting model using deep bidirectional lstm networks," *Energy Conversion and Management*, vol. 234, p. 113944, 2021.
98. L. Zhang, P. Liu, L. Zhao, G. Wang, W. Zhang, and J. Liu, "Air quality predictions with a semi-supervised bidirectional lstm neural network," *Atmospheric Pollution Research*, vol. 12, no. 1, pp. 328–339, 2021.
99. M. M. Rahman, Y. Watanobe, and K. Nakamura, "A bidirectional lstm language model for code evaluation and repair," *Symmetry*, vol. 13, no. 2, p. 247, 2021.
100. A. Onan and M. A. Toçoğlu, "A term weighted neural language model and stacked bidirectional lstm based framework for sarcasm identification," *IEEE Access*, vol. 9, pp. 7701–7722, 2021.
101. M. Kaselimi, N. Doulamis, A. Voulodimos, E. Protopapadakis, and A. Doulamis, "Context aware energy disaggregation using adaptive bidirectional lstm models," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3054–3067, 2020.
102. W. Li, F. Qi, M. Tang, and Z. Yu, "Bidirectional lstm with self-attention mechanism and multi-channel features for sentiment classification," *Neurocomputing*, vol. 387, pp. 63–77, 2020.
103. H. Jahangir, H. Tayarani, S. S. Gougheri, M. A. Golkar, A. Ahmadian, and A. Elkamel, "Deep learning-based forecasting approach in smart grids with microclustering and bidirectional lstm network," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 9, pp. 8298–8309, 2020.
104. Y. Cao, F. Yang, Q. Tang, and X. Lu, "An attention enhanced bidirectional lstm for early forest fire smoke recognition," *IEEE Access*, vol. 7, pp. 154732–154742, 2019.
105. F. Long, K. Zhou, and W. Ou, "Sentiment analysis of text based on bidirectional lstm with multi-head attention," *IEEE Access*, vol. 7, pp. 141960–141969, 2019.
106. 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.
107. S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, "A systematic literature review on phishing email detection using natural language processing techniques," *IEEE Access*, vol. 10, pp. 65703–65727, 2022.
108. J. Zhang and Y. Liu-Thompkins, "Personalized email marketing in loyalty programs: The role of multidimensional construal levels," *Journal of the Academy of Marketing Science*, pp. 1–21, 2023.