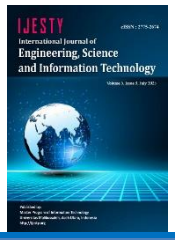
International Journal of Engineering, Science and Information Technology
Volume 5, No. 3 (2025) pp. 337-343
eISSN: 2775-2674
Website: http://ijesty.org/index.php/ijesty
DOI: https://doi.org/10.52088/ijesty.v5i3.1058
Research Paper, Short Communication, Review, Technical Paper



Fake News Detection in Model Integral: A Hybrid CNN-BiLSTM Model

Renuka Nyayadhish[1]*, Chaya Jadhav[2], Ch Bhupati[3], R.A. Mabel Rose[4], M Prabhu[5]

[1]Department of Software Engineering, University of Greater Manchester, RAK Academic Centre, Ras Al Khaimah, UAE
[2]Dr. D.Y. Patil Institute of Technology, Pimpri, Pune, India
[3]Department of IoT, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
[4]Department of Computer Science and Business Systems, Panimalar Engineering College, Chennai, India.
[5]Department of ECE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India

**Corresponding author Email: r.nyayadhish@bolton.ac.uk*

The manuscript was received on 1 February 2025, revised on 10 March 2025, and accepted on 15 June 2025, date of publication 24 June 2025

Abstract

The act of recognizing news that intentionally spreads false information via social media or traditional news sources is known as fake news detection. The characteristics of fake news make it difficult to identify. The spread of fake news and misleading information has increased dramatically due to social media's role as a communication tool and the quick advancement of technology. There is an urgent need for automated and intelligent systems that can differentiate between authentic and fraudulent information due to the fast dissemination of unverified content. The proposed hybrid model efficiently captures regional and worldwide relationships in textual details to address this by combining multiscale residual CNN and BiLSTM layers. The BiLSTM layers manage contextual representations and sequential dependencies, while the CNN layers concentrate on extracting deep local features. The model's capacity to recognize patterns of deception in textual content and comprehend semantic flow is enhanced by this dual architecture. The Edge-IIoT set data and the IoT-23 information from Aposemat were utilized in this study to assess the suggested framework empirically. A concept based on information transfer and sophisticated adaptive systems, we provide an understanding of outliers management paradigm of "generation–spread–identification–refutation" for identifying false information during emergencies. Findings from experiments clearly illustrate the superiority of the BiLSTM approach, demonstrating not only its state-of-the-art efficacy in identifying fake news but also its significant edge over traditional machine learning algorithms. This highlights the BiLSTM approach's critical role in protecting our information ecosystems from the ubiquitous threat of misinformation.

Keywords: *Fake News, Bilstm Approach, Machine Learning, Ecosystems, Misleading Information.*

1. Introduction

The number of people using the Internet has significantly expanded due to the advancement of information and communication technologies. Both newsreaders and news presenters benefit from the ease and speed it brings by switching from traditional to digital information and news consumption. Additionally, the Internet platform produces a lot of bogus news information for convenience. Since fake news possesses the potential to topple authorities and jeopardise modern society, it has emerged as a significant worry [1]. For instance, the term "fake news" gained considerable traction during the 2016 US election campaign as a result of the influence of scammers. One of the most significant sources of online news data is the Internet. The news was no longer printed on paper as it once was. Nowadays, newspaper bureaus use online channels. The Internet makes it simple for readers to obtain information anytime and anywhere. Individuals may now easily share news items on social media platforms like Facebook, Instagram, Twitter, Google, YouTube, Google+, and Line, and they feel at ease accessing news online [2] [3].

Advanced deep learning algorithms have made new approaches to stock price prediction possible in recent years [4]. Convolutional neural networks (CNNs) are good at identifying local characteristics in time-series data but not very good at identifying enduring reliance. Long-term dependencies in time series are well handled by recurrent neural networks (RNNs), particularly long short-term memory (LSTM) networks and gated recurrent units (GRUs). Yao experimented with randomly chosen stocks from the CSI 300 members using the LSTM model and discovered that while the prediction results outperform the other two models in comparison, more helpful information remains untapped.

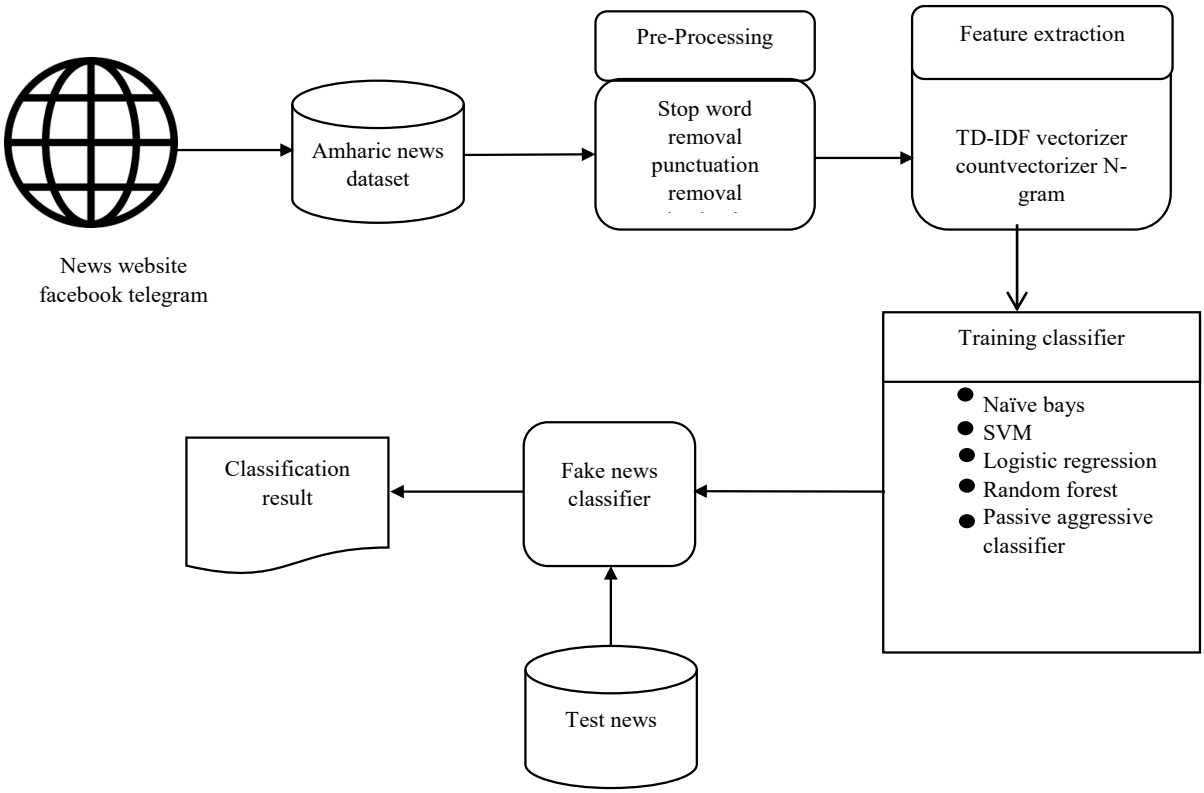


Fig 1. The suggested architecture for detecting fake information

The creation of text-based, complicated algorithms that cover various topics is hindered by the lack of hand-labelled fake news datasets in Figure 1 [5]. The dataset for the phoney news challenge does not meet our needs because it includes the ground truth on the links between texts, but does not specify whether those texts are true or false.

This paper's remaining sections are organised as follows: A summary of pertinent Research on identifying false news is provided in Section 2. Section 3 presents the suggested paradigm and describes our study approach. We provide thorough results on the prediction models' performance, including all other models created for this study, in Section 4. The paper is finally concluded in Section 5.

2. Literature Review

The objective of the current Research is to determine fake news by employing both content-based and contextual methods. Two main categories [6] can be used to organise the characteristics dependent on content employed in this type of Research: generic features and latent features. Commonly utilised in conventional machine learning models, general textual features use statistical methods such as parts-of-speech (POS) tags, including nouns and verbs, to assess syntax and bag-of-words (BoW) models to compute Linguistic prevalence metrics. On the other hand, latent textual features can produce implicit patterns or embeddings at the word, phrase, or document level. Compact vector representations are made using this technique, which can be used for additional analysis.

With about 528.3 million active users, Twitter is a very well-known social networking platform [7]. It has come under heavy fire, along with other social media sites, for helping spread rumours and controversy, especially concerning the COVID-19 pandemic. Although social media significantly boosts awareness, there is growing concern that the combination of misinformation and fake news has exacerbated the global dissemination of false information. Unfortunately, some people use the present pandemic to spread dangerous and false data on social media. The assertion that the "Ivermectin" tablet can treat COVID-19 is an example of false information.

The dissemination of inaccurate information about health on Social media poses a significant problem with wide-ranging effects. Several Research have looked at the works on this topic and discovered a variety of inaccuracies, encompassing conspiracy theories, incorrect claims regarding disease causes, and treatment claims additionally, it has been emphasized how this disinformation impacts people's health, encouraging dangerous health behaviors, eroding confidence in public health authority, and promoting vaccine hesitancy [8]. Public health campaigns, social media platform policies, fact-checking, and artificial intelligence are some strategies suggested to stop the spread of fake news. Nevertheless, these methods have drawbacks and need more investigation and advancement to increase their precision and effectiveness.

The SVM was used for additional classification, while the CNN was employed for feature extraction. With an accuracy of up to 88%, this pairing improved the accuracy results by utilising the advantages of CNN and SVM. However, this model has trouble with longer training times and more sophisticated computations. Random forest (RF) algorithms and hybrid SVMs were suggested [9] to enhance evaluation metrics for identifying false news. The researchers demonstrated that their prototype performed better than other conventional ML classifiers with an accuracy of 97.56% and an F1-score of 93.50%. This model's efficiency and quick training times are its defining features.

Our structure offers a more comprehensive comprehension of the textual information by considering several factors simultaneously, improving the detection process. Furthermore, we suggest using context-aware representation models to encode the input text, like BERT [10]. Using BERT and its contextual knowledge-capturing capabilities adds insight to our methodology, improving its efficacy in

identifying false information. To assess the performance of our system, we experiment with two distinct kinds of textual depictions for news articles: Pre-trained embedding models that are context-independent, such as BERT, and context-aware, such as GloVe.

3. Methods

3.1. Long short-term memory

Recurrent neural networks (RNNs) are networks with some degree of future prediction ability. Extended-duration series cause the RNN to develop into an intense network, even though simple RNNs are good at predicting time series and handling other sequences. By using memory cells with an arbitrary quantity of temporal data, the LSTM, a component of the RNN [11], can resolve the issue of disappearing gradients.

The LSTM has a three-step process that includes an output stage, a memory stage for choosing, and a forgetting stage. The LSTM has one or more explicit layers and two communicated states, a c^t and an h^t. Four distinct, completely connected layers receive the present input vector x^t and the preceding short-term state [12] h^{t-1}. A sigmoid activation function multiplies the splice vectors by a weight matrix and then converts z^o to a value between 0 and 1 as a gate state. The following is the LSTM internal message-passing formula:

$$z^f = \sigma\left(W_{xf}x^t + W_{hf}h^{t-1} + b_r\right) \quad (1)$$

$$z^i = \sigma(W_{xi}x^t + W_{hi}h^{t-1} + b_i) \quad (2)$$

$$z = tanh(W_z x^t + W_{zi}h^{t-1} + b_z) \quad (3)$$

$$h^t = z^o \times tanh(c^t) \quad (4)$$

$$y^t = \sigma(W'h^t) \quad (5)$$

Where σ [?] stands for the sigmoid activation function, the bias vector, and the weight matrix between various nodes.

3.1.1. Attention-mechanism

Hybrid modelling and attention techniques are used in many areas, such as visual computing, time series prediction, natural language processing, and more. In several financial quantisation areas [13], CNN-BiLSTM has also been successfully used with a system of attention that adaptively captures long-range dependencies between items by determining their proportional significance [14].

The correlation data can be described as $Xt, Xt-1, \ldots, Xt-n$ model inputs. The following is the precise weighted total output:

$$a_i = Softmax(s_i) = \frac{e^{s_i}}{\sum_{j=1}^{L_x} e^{s_i}} \quad (6)$$

$$s_i = V_s^T tanh(W_{ls}H_t^s) \quad (7)$$

Where H_t^s represents the BiLSTM hidden layer's output, W_{ls} represents its associated weight, and V is the learnable parameter [15].

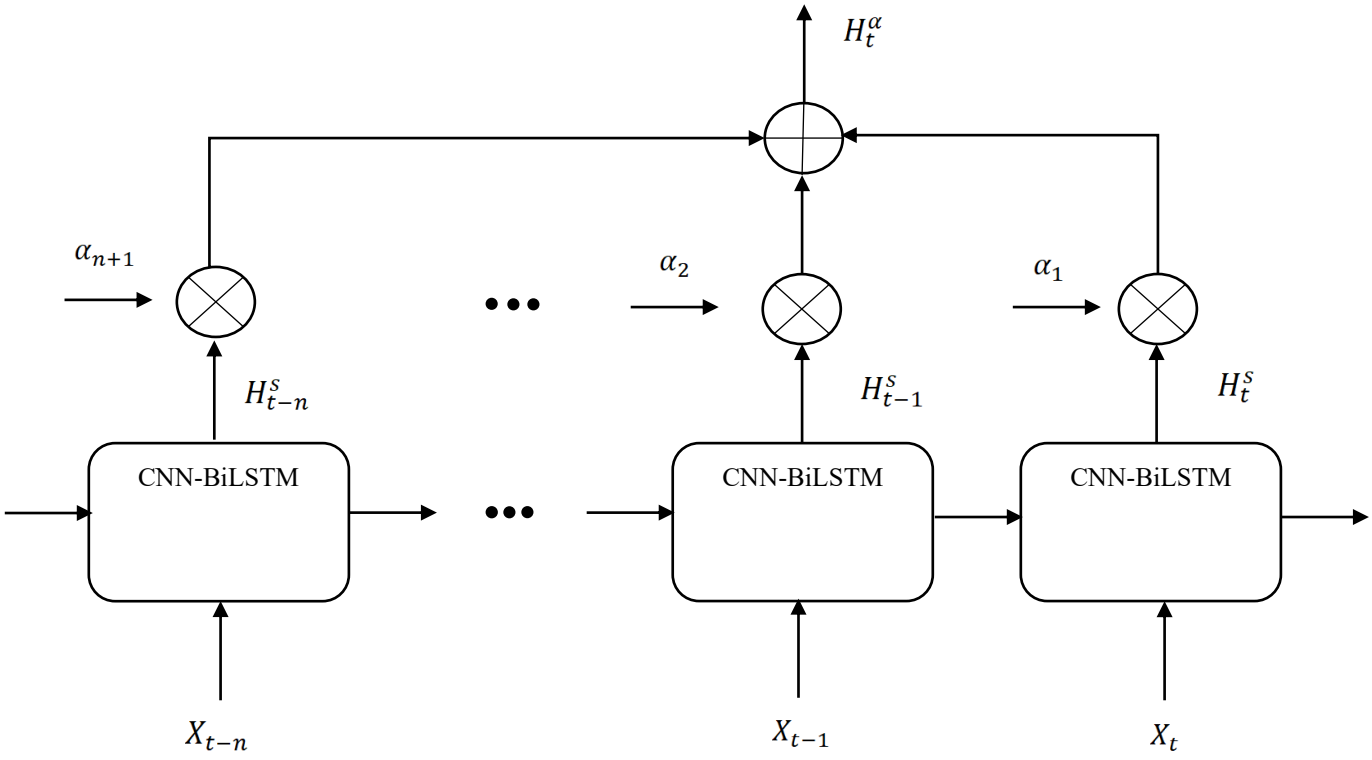


Fig 2. Structure of the self-attention mechanism

In several financial quantisation areas [16] [18], CNN-BiLSTM has also been successfully used with a system of attention that adaptively depicts the long-term relationships between items by determining their proportional significance. Figure 2 displays the attentional mechanism model.

3.2. Future Framework

A framework for defending IoT networks against different types of assaults is presented in this section. Three neural network models—a "CNN, a BiLSTM network, and a fully connected DNN" are powerfully combined to form the framework's foundation, as shown in Figure 3. Together, these models create a strong CNN–BiLSTM–DNN model. As seen in Figure 4, the CNN model's retrieved features will be sent into the BiLSTM model for additional processing [17].

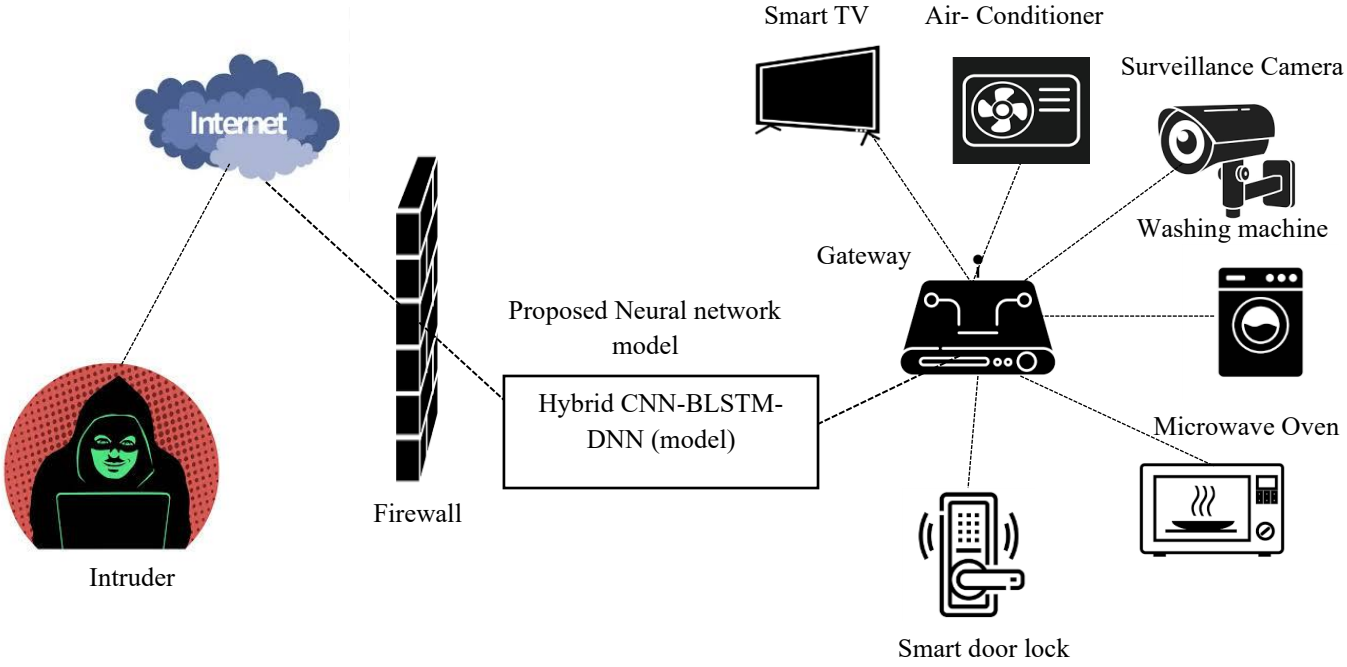


Fig 3. Proposed architecture

The BiLSTM model outcome will be forwarded to the DNN for ultimate categorisation. With the device's address and identity, the system will notify the monitor if the DNN determines the feature is harmful. By doing this, the system can eliminate the malicious gadget and its operations, among other precautionary actions [19] [20]. By adding a layer of temporal comprehension to the feature extraction method, the BiLSTM approach used in our suggested model aids in identifying temporal patterns in the data. This enables the model to better recognise and react to changing threats by learning and remembering patterns that emerge over time. This aids in the DNN's ability to classify data more accurately, particularly when handling harmful behaviours that entail a sequence of occurrences.

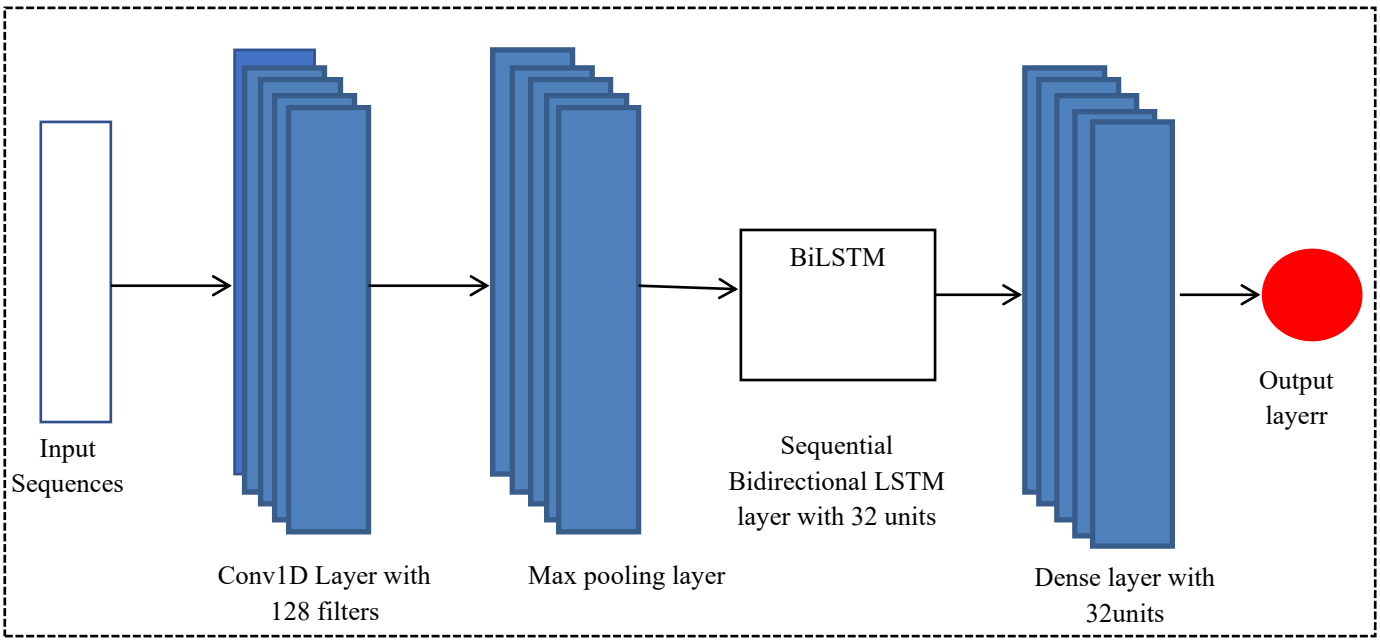


Fig 4. Hybrid model structure

After that, the DNN will get the output from the BiLSTM model for ultimate classification. The system will notify the tracking device of the device's address and identity if the DNN determines that the feature is harmful. As a result, the system can take preventative actions, such as cutting off the unwanted device and its operations. By adding a level of temporal comprehension to the feature extraction method, the BiLSTM model in our suggested model helps capture the temporal connections in the data. This enables the model to recognise and recall patterns that emerge over time and enhances its ability to identify and react to emerging threats. This aids in the DNN's ability to classify data more accurately, particularly when handling harmful behaviours that entail a sequence of occurrences.

3.3. Dataset Preparation

The Edge-IIoT set data and the IoT-23 information from Aposemat were utilized in this study to assess the suggested framework empirically. In the IoT-23 dataset, network traffic from three IoT devices—a Philips HUE bright LED lamp, the Amazon Echo intelligent team member, and a Somfy intelligent door lock—is recorded in 20 malware rounds from infected and benign situations. This dataset was obtained from the "Stratosphere Laboratory Science, AIC group, FEL, CTU college, Czech Republic, and includes network traffic from the Internet of Things". Several gadgets, procedures, sensors, and cloud/edge combinations are present in this testbed. Data were gathered using more than ten Internet of Things devices, including inexpensive digital sensors for temperature and humidity tracking, ultrasonic sensors for pH gauges, water level detection devices, cardiovascular tracks, soil moisture sensors, and flame sensors.

3.4. Input Layer

This layer accepts raw data and prepares it for further layers to process. Time-series sequences representing developed network traffic properties, including package size, flow time frame, and protocol types, are created from the prepared IoT network traffic information received at this layer. The number of characteristics determines the fixed length of each sequence.
The input of the model is shown as a time-lapse matrix with the following form:

$$X \in R^{N \times T \times F} \quad (8)$$

T is the number of time increments in each cycle, F is the number of characteristics (e.g., package size, flow time frame, protocol kinds), and N is the sample size. Here is a representation of each input sequence:

$$X_i = \{x_1, x_2, \ldots, x_3\}, X \in R^F \quad (9)$$

3.5. 1D Convolution Layer

Spatial features are extracted from some areas of the input data using the convolutional layer. In this investigation, just one convolutional layer is employed. One hundred twenty-eight filters with a kernel number of 5 and ReLU activation are used in the Conv1D layer. The activation function of ReLU, which is incorporated at the Conv1D layers to decode complex data patterns, introduces non-linearity. Following the application of the ReLU activation function, the Conv1D layer's output for a given input X is as follows:

$$Y_{ijk} = ReLU\left(\sum_{j=0}^{F-1} X_{I,J+L}.w_{L,K} + b_k\right) \quad (10)$$

In batch I, where position $j+l$ in the sequence is the input value, l indicates the filter locations, and $Xi,j+l$, the weight at the n-th position of the k-th filter is represented by Wl,k. In contrast, the bias term for the k-th filter is defined by bk. ReLU(z)=max(0,z) is the activation function, applied element-wise to introduce non-linearity, with $1l$=0 summation over the filter size F. In this instance, the output is at batch index i, position j, and filter k.

4. Results and Discussion

There are 13,816 records evenly split across each group. Training, validation, and test sets are the three categories into which we divided the data. There were 20,310 training data points available. Twelve thousand four hundred thirty-five test data points and 8,704 validation data points were used. An example of data gathered to develop machine learning for detecting fake news is displayed in Table 1. Test, validation, and training sets are shown in Table 2.

Table 1. Sample data collected

Labels	No. samples
False	13,816
Real	13,816
Doubtful	13,816
Total	41,448

Table 2. Training, validation, and test sets

Datasets	No. samples	Ratio
Training	20,721	0.50
Validation	8282	0.20
Text	12,445	0.30
Total	41,448	1.00

Score fake, score real, sim matched, domain fake, and domain genuine are highlighted in Table 3. The classes that are targeted include suspicious, legitimate, and fake.

Table 3. Correlation of feature data

	Score Fake	Score Real	Sim Matched	Domain Fake	Domain Real	Fake	Real	Suspicious
Score Fake	1.00	0.07	0.33	0.92	0.16	0.70	-0.43	-.035
Score Real	0.07	1.00	0.15	0.10	0.86	0.04	0.15	-0.22
Sim Matched	0.33	0.15	1.00	0.35	0.22	0.24	0.30	-0.65
Domain Fake	0.91	0.10	0.37	1.00	0.20	0.76	-0.47	-0.36
Domain Real	0.16	0.86	0.20	0.22	1.00	0.11	0.11	-0.25
Fake	0.60	0.05	0.27	0.24	0.11	1.00	-0.62	-0.49
Real	-0.42	0.16	0.30	0.24	0.11	-0.62	1.00	-0.36
Suspicious	-0.33	-0.20	-0.63	-0.47	-0.25	-0.49	-0.35	1.00

Notably, there is a correlation between the targets and the retrieved features. Both the false and real classes had a favourable connection to the simulation, which was matched. False class has a predictive influence on score fake and domain fake characteristics, which have 0.7 and 0.76, respectively. A positive connection exists between the class real and score real and domain real characteristics of 0.16 and 0.11, respectively. It suggests that the data can accurately depict both fictitious and actual courses. However, there is a negative association between characteristics and class suspicion. Making a distinction between the suspicious group would be challenging.

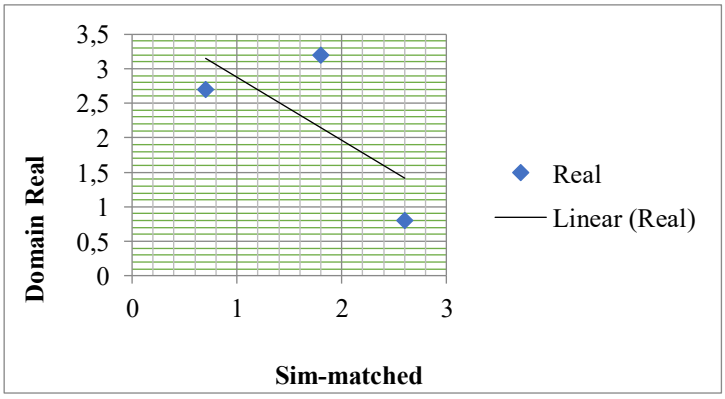


Fig 5. The clustered feature data's scatter joint plot

The data with clustered features in a scatter joint plot is displayed in Figure 5. As the data clustering demonstrates, building a classifier to distinguish between the three classes is feasible. Class phoney appears distinct from the others, although suspicious and real, and shares some traits.

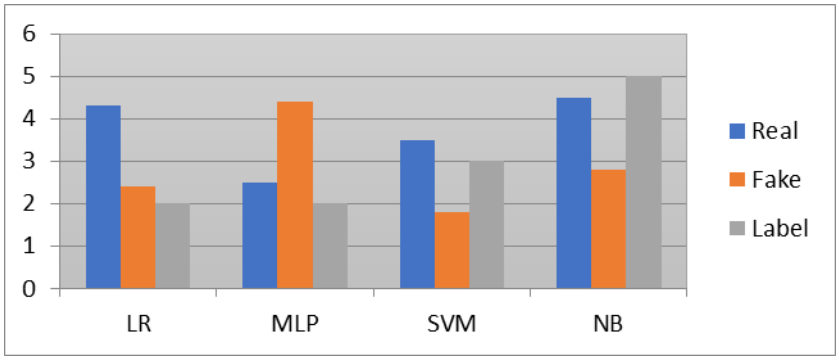


Fig 6. Box plot showing machine learning test accuracy

A box plot based on a 10-fold cross-validation test accuracy is displayed in Figure 6. It confirms that the best system for attaining a flawless accuracy score was LSTM. A deep learning LSTM model produces the best outcomes regarding accuracy, recall, reliability, and F-measure; these metrics are 1.00.

The data from fake news is highly dynamic. Developing a fake news detection algorithm that can generalise all data that is not visible is a challenging issue. We will use online and social media news data by feeding it into a classifier. As was mentioned during the data preparation phase, we retrieved the data containing both authentic and fraudulent news using web crawlers to retrieve information. The feature extraction step gathers news data for five features using the fake news domain length, real news domain length, similarity matching, and false news score.

5. Conclusion

The dynamic nature of news stories makes it challenging to identify fake news. The investigation suggests a fresh, effective strategy to combat false information. As part of our methodology, we first employ data to get data from an internet news source and social media.

We will investigate deep learning models more in subsequent studies. Our research question is how to make deep learning comprehend the news more like humans. The algorithm can identify the kind of news and explain its response. Additionally, the machine must accurately assess and react to news content, including text, sound, and video. We also intend to use Research to gain a deeper comprehension of the language. A more intricate architecture, like BERT and GPT, will be required. That offers room for additional Research in the future.

References

[1] H. Xia, Y. Wang, J. Z. Zhang, L. J.Zheng, M. M. Kamal, & V. Arya, "COVID-19 fake news detection: A hybrid CNN-BiLSTM-AM model," Technological Forecasting and Social Change, vol. 195, pp. 122746, 2023.

[2] Y. Zhou, Y. Yang, Q. Ying, Z. Qian, and X. Zhang, "Multi-modal fake news detection on social media via multi-grained information fusion," *arXiv preprint arXiv:2310.10840*, 2023.

[3] A. K. Ghoshal, N. Das, S. Das, and S. Dhar, "Minimizing spread of misinformation in social networks: A network-topology based approach," *Soc. Netw. Anal. Min.*, vol. 15, no. 15, pp. 1–13, 2025.

[4] A. B. Alawi, & F. Bozkurt, "A hybrid machine learning model for sentiment analysis and satisfaction assessment with Turkish universities uses Twitter data," Decision Analytics Journal, vol. 11, pp. 100473, 2024.

[5] J. Luo, Y. Cao, K. Xie, C. Wen, Y. Ruan, J. Ji & W. Zhang, "Hybrid CNN-BiGRU-AM Model with Anomaly Detection for Nonlinear Stock Price Prediction," Electronics, vol. 14, no. 7, pp. 1275, 2025.

[6] A. U. Hussna, M. G. R. Alam, R. Islam, B. F. Alkhamees, M. M.Hassan & M. Z. Uddin, "Dissecting the infodemic: an in-depth analysis of COVID-19 misinformation detection on X (formerly Twitter) utilizing machine learning and deep learning techniques," Heliyon, 2024.

[7] B. Farhoudinia, S. Ozturkcan & N. Kasap, "Fake news in business and management literature: a systematic review of definitions, theories, methods and implications," Aslib Journal of Information Management, vol. 77, no. 2, pp. 306-329, 2025.

[8] N. Alabid & H. A. Taher, "Enhancing Arabic fake news detection with a hybrid MLP-SVM approach and Doc2Vec embeddings," 2024.

[9] E. Choi, J. Ahn, X. Piao & J. K. CroMe Kim, "Multimodal Fake News Detection using Cross-Modal Tri-Transformer and Metric Learning," arXiv preprint arXiv: vol. 2501, pp. 12422, 2025.

[10] X. Chen, Y. Chen, Y. Liu & J. Pan, "TMEF-BI: Trusted Multimodal Evidential Fusion Considering Behavior Information for Fake News Detection," IEEE Transactions on Computational Social Systems, 2025.

[11] J. Fang, K. Ma, Y. Qiu, K. Ji, Z. Chen & B. Yang, "SEN-CTD: semantic enhancement network with content-title discrepancy for fake news detection," International Journal of Web Information Systems, vol. 20, no. 6, pp.603-620, 2024.

[12] A. Z. Ala'M, M. A. Hassonah, L. Al-Qaisi, R. Qaddoura, B. Al-Ahmad, M. Habib & A. Z. Ala'M, "An Evolutionary Embedded Model Fake News Detector Using an Optimized Support Vectors Machines,".

[13] W. Chen, W. Hussain, F. Cauteruccio & X. Zhang, "Deep learning for financial time series prediction: A state-of-the-art review of standalone and hybrid models," CMES-Computer Modeling in Engineering and Sciences, 2023.

[14] X. Zhao, Y. Liu & Q. Zhao, "Generalized loss-based cnn-bilstm for stock market prediction," International Journal of Financial Studies, vol. 12, no. 3, pp. 61, 2024.

[15] H. Li, & J. Hu, "A hybrid deep learning framework for stock price prediction considering the investor sentiment of online forum enhanced by popularity," arXiv preprint arXiv: vol. 2405, pp. 10584, 2024.

[16] A. Li, J. Chen, X. Liao, and D. Zhang, "Adaptive learning of consistency and inconsistency information for fake news detection," *arXiv preprint arXiv:2402.01230*, 2024.

[17] M. K. Jain, D. Gopalani, and Y. K. Meena, "Hybrid CNN-BiLSTM model with HHO feature selection for enhanced fake news detection," *Soc. Netw. Anal. Min.*, vol. 15, no. 43, pp. 1–11, 2025.

[18] X. Shen, M. Huang, Z. Hu, S. Cai, and T. Zhou, "Multimodal fake news detection with contrastive learning and optimal transport," *Frontiers in Computer Science*, vol. 18, no. 2, pp. 1–13, 2024.

[19] B. Cao, Q. Wu, J. Cao, B. Liu, and J. Gui, "ERIC-FND: External reliable information-enhanced multimodal contrastive learning for fake news detection," in *Proc. AAAI Conf. Artif. Intell.*, vol. 39, no. 4, 2025, pp. 3294–3302.

[20] L. Feng, W. Zhang, and Y. Liu, "SARD: Fake news detection based on CLIP contrastive learning and semantic alignment," *J. Inf. Secur. Appl.*, vol. 80, pp. 103622, 2024.