Leveraging NLP and Sentiment Analysis for ML-Based Fake News Detection with Big Data

AJAY BABU KAKANI[1], SRI KRISHNA KIREETI NANDIRAJU[2], SANDEEP KUMAR CHUNDRU[3], SRIKANTH REDDY VANGALA[4], RAM MOHAN POLAM[5], BHAVANA KAMARTHAPU[6]

[1]Wright State University, USA
[2]University of Illinois at Springfield, USA
[3]University of Central Missouri, USA
[4]University of Bridgeport, USA
[5]University of Illinois at Springfield, USA
[6]Fairleigh Dickinson University, USA

Abstract: As a critical cybersecurity tool, Natural Language Processing (NLP) provides an automated the quick dissemination of misleading information online, necessitating the use of a fake news detecting system. The suggested fake news detection system incorporates sentiment analysis with a number of machine learning (ML) and deep learning models, such as Random Forest (RF) and Logistic Regression (LR) algorithms, Decision Tree (DT), K-Nearest Neighbors (KNN), Support Vector Machine (SVM), and Naive Bayes (NB), in addition to a Long Short-Term Memory (LSTM) neural network solution. The study involved extensive data preprocessing, TF-IDF, and Bag-of-Words feature extraction. The model was then evaluated using binary cross-entropy loss, accuracy and precision, recall, and F1-score assessments. Through efficient sequential and contextual text processing, the LSTM model outperformed other models in the Kaggle fake news dataset, which had over 26,000 items. In experimental evaluation, LSTM outperformed the convolutional neural network (CNN) and Extreme Gradient Boosting (XGBoost) models, achieving 95.1% accuracy, 94.4% precision, 95.3% recall, and 94.2% F1-score. LSTM deep learning (DL) algorithms demonstrate exceptional reliability in identifying deceptive content because they perform better than traditional machine learning methods, thus offering great potential as a basic cybersecurity tool to stop misinformation spread.

Keywords: *Fake news detection, Cybersecurity, Natural Language Processing, sentiment analysis, machine learning, LSTM, TF-IDF, Bag-of-Words.*

Received: June 17, 2025. Revised: July 25, 2025. Accepted: August 13, 2025. Published: September 4, 2025.

1. Introduction

News articles feature sentimental and eloquent words from people involved in the events they depict, it demonstrates a deep emotional connection. Sentiment analysis, a technique used in natural language processing (NLP), looks for and extracts subjective material in text in addition to the emotional expression of news articles [1][2]. In addition to helping news organizations monitor public opinion on a range of problems throughout time, this may be helpful in determining how people feel about a specific topic or event.

The job of determining whether assertions in news are true is known as automated fake news detection. Given the significant social and political effects that social media and traditional news media have on every member of society, this is a novel but crucial NLP topic [3]. Fake news even relates to real-world violent events that threaten public safety. One significant use of NLP in the globe is the detection of false news, which has wider implications for how technology might assist verify the accuracy of claims and inform the public [4]. Asking experts, such as journalists, to verify statements against evidence derived from previously stated or documented facts is the standard approach to this assignment. Automated fake news identification on online material has drawn attention from the AI research field due to the continuously expanding Internet community and the pace at which information is spreading [5].

The identification of fake news is difficult, and research on the subject is still in its early stages. However, the spread of false news is increasing, necessitating more study and the investigation of novel avenues to enhance the methods for spotting it. Numerous research on spotting false news on social media rely on one or more characteristics, such user behaviour, network propagation, or content [6]. Analyzing user comments to determine their opinions about the news may be crucial in spotting fake news and providing insight into the veracity of the material that is released. Asserted that user comments, where mood or emotion expression is essential, had significant discriminating value in identifying bogus news [7]. These user-generated inputs may be processed and scaled across platforms by utilizing Big Data technology. This improves ML models for detecting bogus news and enables more precise sentiment analysis [8].

The detection of fake news greatly depends on Big Data because it handles whole volumes of news content together with user interactions from social media in real time for analysis. Through combining Big Data technologies with NLP and machine learning systems gain higher capabilities to find patterns and detect irregularities and improve their accuracy levels [9][10]. Handling large amounts of data is essential because it provides effective solutions for tracking the dynamic and widespread spread of fake news content.

The investigation and analysis for ML algorithms for false news detection highlight a number of unexplored research topics [11]. The first significant gap in the existing body of research concerns comparative analysis studies comparing various machine learning techniques, particularly those that include Empath, term frequency inverse document frequency (TF–IDF), and a hybrid model that blends the two. Apart from contrasting various machine learning models, there is a deficiency in investigating transfer learning uses of the Bernoulli naive Bayes (BNB) classifier in the context of identifying false information [12]. Finally, there hasn't been enough research done on using incremental learning with the

multinomial naive Bayes (MNB) and BNB classifiers for false news identification.

1.1 Significance and Contribution of Paper

The detection method demonstrated great value because it enhances fake news detection in cybersecurity through sophisticated NLP combined with sentiment analysis methodologies. The growing amount of false information online demands trustworthy detection models, especially when the content targets cybersecurity knowledge bases. The research builds this knowledge through the combination of LR, traditional classifiers, and NB, along with LSTM as more complex models to define which methods work best for identifying fake news. This proposed methodology delivers a strong framework for solving crucial modern information system challenges owing to its entire methodology that includes data preprocessing and feature extraction and performance evaluation. The research introduces three fundamental contributions which make up its main findings:

- The study integrates advanced NLP and sentiment analysis techniques to improve fake news detection in the cybersecurity domain, enhancing the accuracy of distinguishing misleading information.
- The research uses a systematic strategy that tests three classification models, namely CNN, XGBoost, and LSTM, to discover the optimal solution for fake news detection.
- The investigation implements reliable preprocessing operations and diverse extraction techniques, starting from tokenization and lemmatization, moving toward stop word elimination, and moving toward Bag of Words and NLP models to transform unstructured text into machine learning processable inputs.
- This study conducts a comparative assessment of model based on common assessment criteria, such as F1-score, recall, accuracy, and precision, and loss for determining fake news detection effectiveness.

1.2 Novality and Justification

This study introduces sentiment analysis together with cutting-edge NLP methods to make traditional and DL models particularly LSTM work better for cybersecurity-aware fake news detection. This research adds emotional tone and polarity signals to complement traditional text-based features because they help the model understand the content better. This research investigates multiple ML approaches and LSTM to perform an extensive deep learning evaluation of identifying complex linguistic patterns. This multi-model approach, combined with thorough preprocessing and feature extraction, justifies the methodology's ability to deliver more accurate, reliable, and context-aware fake news detection, making it highly relevant in today's digital misinformation landscape.

1.3 Structure of the paper

The study is structured as follows: Section II discusses pertinent research on cybersecurity fake news detection. Section III explains the steps, approach, and resources utilized. The section IV provides an analysis of the experimental results and a description of the suggested system. Section V outlines the findings and upcoming projects.

2. Literature Review

This section outlines of the literature on sentiment analysis and natural language processing in machine learning-based false news identification for cybersecurity applications.

Karthika, Murugeswari and Manoranjithem (2019) the online store Flipkart.com's rating is analyzed and classified as either positive, neutral, or negative based on the product's attributes. After calculating their accuracy, precision, F-measure, and recall, the RF and SVM approaches are compared for accuracy. whereby the RF achieves 97% accuracy, outperforming the SVM [13].

Yadav and Bhojane (2019) suggest methods for doing sentiment analysis on Hindi multidomain reviews with input text files encoded in UTF-8 using the Devanagari script. The accuracy of each method is finally reported, and various domain review datasets are manually and randomly gathered. They include words that they have created a dictionary for in Mix-Hindi, such as "brave," "careful," "mineral," and etc. Approach 1 obtains an overall accuracy of 52%, whereas approaches 2 and 3 reach 71.5% and 70.27% accuracy, respectively [14].

Qawasmeh, Tawalbeh and Abdullah (2019) One of the most difficult problems with the current content-based analysis of conventional techniques is identifying false news. Additionally, provide an automated method for identifying false information by utilizing contemporary ML techniques. When applied to the proposed model, a bidirectional LSTM concatenated model, achieves 85.3% accuracy on the FNC-1 dataset [15].

Kaliyar, Goswami and Narang (2019) The experiments in this article have employed a tree-based Ensemble ML framework with optimized parameters that integrates content and context level data for the identification of fake news. Comparing experimental findings to current benchmark results shows how successful the ensemble framework is. 86% accuracy was attained in the multi-class classification of bogus news using four classes using the Gradient Boosting technique [16].

Aksu and Ali Aydin (2018) Cyberterrorism is one of the most significant threats facing the globe today, depending on these difficulties. In order to prevent cyberattacks, intrusion detection systems, or IDS, were created. Using the new CICIDS2017 dataset, this study employed DL and SVM methods to identify port scan attempts. Accuracy rates of 97.80% and 69.79% were attained, respectively [17].

Table I below shows the literature review summary of Fake News Detection in Cybersecurity various studies, approaches, datasets, main conclusions, limits, and directions for further research.

TABLE I. SUMMARY OF LITERATURE REVIEW BASED ON NLP AND SENTIMENT ANALYSIS FOR ML

Author	Methodology	Dataset	Key Findings	Limitations	Future Work
Karthika, et al. (2019)	Random Forest and SVM classifiers	Flipkart product reviews	Random Forest achieved highest accuracy (97%)	Limited to only two ML models; lacks deep learning comparison	Use of deep learning models like BERT or

	implemented in SPYDER		over SVM for sentiment classification		LSTM for enhanced accuracy
Yadav, et al. (2019)	NN-based prediction using pre-classified words/sentences and Hindi SentiWordNet (HSWN)	Hindi multi-domain reviews (UTF-8 encoded, with Mix-Hindi words)	Achieved 52% (approach 1), 71.5% (approach 2), 70.27% (approach 3) accuracy	Performance affected by ambiguous words and Mix-Hindi vocabulary	Expand lexicon and integrate contextual embeddings for Hindi sentiment
Qawasmeh, et al. (2019)	Bi-directional LSTM model	FNC-1 dataset	85.3% accuracy in identifying false news was attained.	Limited to one dataset; lacks comparative study with transformer models	Integrate transformer-based models and real-time data handling
Kaliyar, et al. (2019)	Gradient Boosting in an Ensemble ML framework	FNC (multi-class fake news dataset)	Achieved 86% accuracy in four-class fake news classification	Lack of real-time processing and limited external validation	Implement real-time fake news detection with more robust features
Aksu, et al. (2018)	Deep Learning and SVM for port scan detection	CICIDS2017 dataset	Achieved 97.80% accuracy (DL) and 69.79% (SVM)	Dataset may not reflect emerging attack patterns	Develop adaptable IDS models for new cyber-attack patterns

3. Methodology

The purpose of this work is to use sentiment analysis and NLP techniques to ML-based fake news identification in the cybersecurity domain in order to improve the accuracy and reliability of identifying false information. To do this, a systematic strategy based on the LSTM model is employed, as seen in Figure 1. The process begins with the collection and exploration of a fake news dataset through data analysis and visualization. Textual content cleaning takes place through regular expression applications and tokenization as well as stop word elimination with lemmatization to prepare data for analysis. The text undergoes processing through both Bag of Words and NLP-based representation models that convert unstructured text data into a structured format. The training and testing operations occur after breaking up the processed data while the LSTM model conducts training before evaluation. The system evaluation requires parameters to assess how well it detects bogus news, including as accuracy, precision, recall, F1-score, and loss. The proposed methodology appears as Figure 1 which depicts its flowchart design.

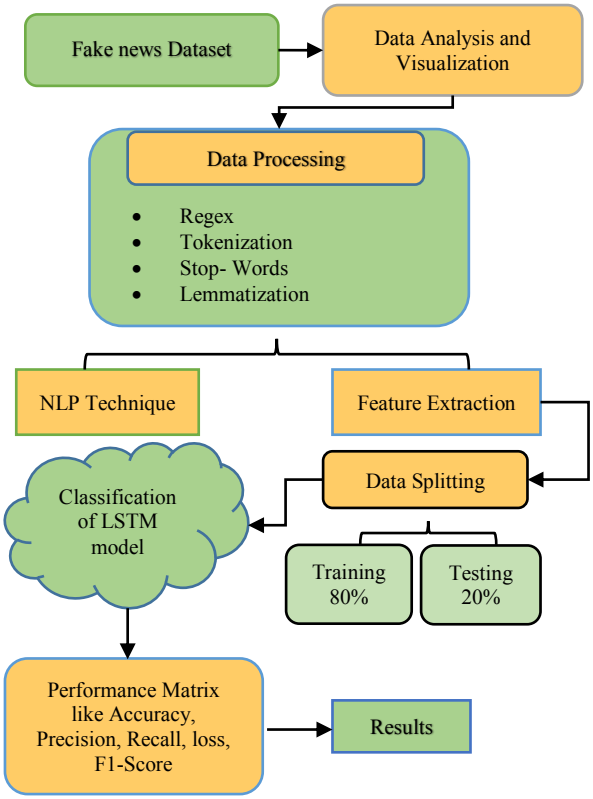


Fig. 1. Flowchart illustrating the process of detecting fake news in cybersecurity

The following is a quick description of the flowchart's steps:

3.1 Data Analysis and Visualization

The Kaggle fake news dataset is employed to develop the detection framework. This dataset, compiled through automated web scraping from various search engines, contains a diverse collection of 26,000 unique news articles from multiple news portals and social media platforms. Originally released as a data science community challenge, it has been successfully utilized in previous research. The dataset features four primary columns: the article's title, the author's name, and a special identification, and the main text content. Additionally, the training set includes a classification column indicating whether each news item is reliable or potentially unreliable. The text column contains 20,822 unique entries, providing substantial variety for robust model training and evaluation.

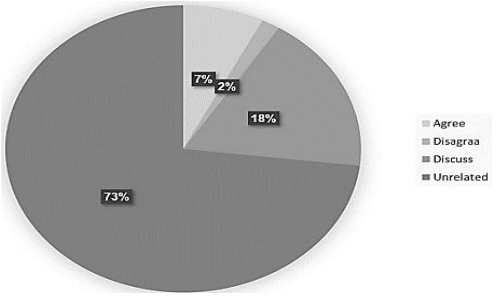
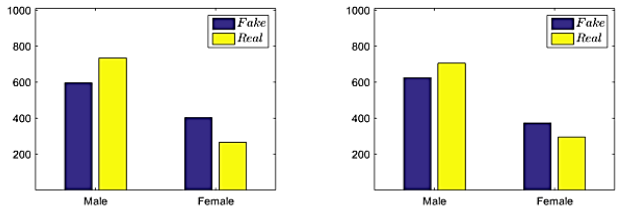


Fig. 2. Data Classes Distribution Rate in Fake News Detection

Figure 2 displays the distribution of response types in what appears to be a discussion analysis. The largest segment is labeled "Unrelated" at 73%, indicating that nearly three-quarters of the responses were off-topic. The remaining segments show "Discuss" at 18%, "Disagree" at 7%, and "Agree" at just 2%. The legend on the right identifies these four categories with different gray shades. This visualization suggests that in the analyzed discussions, most contributions did not directly address the topic at hand, while genuine engagement through discussion, agreement, or disagreement collectively represented only 27% of the responses.



(a) BuzzFeed (b) PolitiFact

Fig. 3. Gender Distribution of Fake News Dataset

Figure 3 displays two bar graphs from BuzzFeed and PolitiFact comparing fake (purple) versus real (yellow) content by gender. Both graphs show similar patterns: males have higher overall counts than females, with real content exceeding fake for males. Conversely, for females, fake content exceeds real content. The y-axis ranges from 0-1000, with male values generally higher (500-700) than female values (250-400).

3.2 Data Preprocessing

Preprocessing is essential for getting textual data ready for ML since it ensures consistency and removes noise. This work employs a range of methods such as regex-based cleaning, tokenization, stop word elimination, lemmatization, and converts the unstructured text into a format appropriate for model training, using TF-IDF. The applied techniques are discussed in detail below:

- **Regex:** Regex is used to eliminate punctuation from text data. Exclamatory signs and other superfluous punctuation are frequently found in phrases. To eliminate these unnecessary punctuation marks and make the dataset noise-free, use regex. Grammar without context is the foundation of Regex.
- **Tokenization:** Sentences are broken up into words using a preprocessing method called tokenization.
- **Stop Words:** To reduce noise, increase the model's speed and effectiveness, and conserve memory, the English stop words library is used in the preprocessing procedure model data.
- Lemmatization: In order to handle data ambiguity and inflection, lemmatization is utilized to convert words into root words.

3.3 Feature Extraction with TF-IDF

In fake news detection, feature extraction from news content involves deriving discriminative attributes from both linguistic and visual modalities. Linguistic features are obtained from the headline and body text, capturing stylistic, syntactic, and semantic cues that reflect deceptive writing patterns. TF-IDF feature extraction to enhance fake news detection in cybersecurity. An LSTM model is implemented to classify misinformation with improved accuracy and reliability, which is expressed as Equation (1):

$$TF - IDF = TF_{td} \,.\, IDF_t \tag{1}$$

where t represents the documents and t is a word. The statistic known as phrase frequency, or TF for short, measures how frequently a phrase appears in a document. Equation (2) is thus used to measure phrase frequency TF.

$$TF = \frac{q_{td}}{Number\ of\ terms\ in\ the\ document} \tag{2}$$

In this q is the number of times the term "t" appears in the document "d.". Inverse document frequency, represented by the symbol IDF, shows how important a phrase is. The IDF Equation (3).

$$IDF = \frac{\log(1+n)}{(1=df)_{dt}} + 1 \tag{3}$$

The denominator here is the document frequency of the word, t, whereas n is the number of documents.

3.4 Data Splitting

The experimental setup, an 80:20 split was used for the purpose of dividing the information into research and evaluation sets. This approach ensured effective model training while reserving sufficient data for evaluating predictive performance.

3.5 Classification of LSTM Model

A specific kind of RNN called LSTM was created to get over the drawbacks of conventional RNNs, especially the short-term memory problem. A process known as the cell state, which permeates the whole chain with just slight linear interactions, allows LSTM networks to store information for extended periods of time [18]. By allowing gradients to run unaltered, this structure resolves the vanishing gradient issue that conventional RNNs frequently encounter. The LSTM architecture's forget gate establishes how much of the previous cell state should be retained. The Equation (4) defined as:

$$f_t = \sigma\,(W_f.[h_{t-1}, x_t] + b_f) \tag{4}$$

Here, f_t is at time t, the forget gate vector was calculated using the sigmoid activation function. The concatenated vector of the prior hidden state h_{t-1} is used and current input x_t, multiplies it with weights W_f, adds bias b_f, and squashes the result between 0 and 1 to determine whether data from the prior cell state should be discarded. A general neural network design based on LSTM is depicted in Figure 4.

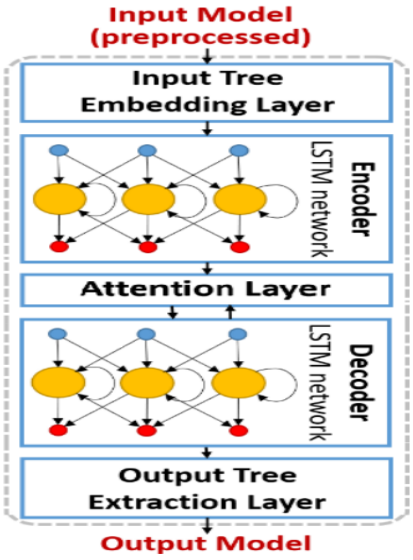


Fig. 4. The Architecture of LSTM model

Alongside the input and forget gates determine what fresh data should be kept in the cell state. It works in conjunction with a candidate vector $\hat{c}_t$, which proposes new ideals that the state may incorporate. These two vectors update the cell state C_t, blending old memory with new input. The Equation (5), (6) and Equation (7) shows as follow:

$$i_t = \sigma(W_t.[h_{t-1}, x_t] + b_i \quad (5)$$

$$\hat{c}_t = tanh(W_c.[h_{t-1}, x_t] + b_c) \quad (6)$$

$$C_t = f_t * C_{t-1} + i_t * \widehat{C_t} \quad (7)$$

The updated cell state C_t is a weighted combination of an earlier condition C_{t-1} (controlled by the forget gate f_t) and the new candidate values C_t (scaled by the input gate i_t). The LSTM system maintains two processing components, which enable it to control which information gets memorized and forgotten, thus achieving durable knowledge retention.

The output gate determines which aspects of the cell state data are used to generate the output. The new hidden state h_t calculated during the current time step functions both as a representation of the past information and as the output for the same time frame. The h_t value results from applying the sigmoid gate to a tanh activation of the recently modified cell state. Equation (8) and (9) are defined as follows:

$$o = \sigma(W_o.[h_{t-1}, x_t] + b_o) \quad (8)$$

$$h_t = ot * \tanh(C_t) \quad (9)$$

The operation on h_t flows to both succeeding LSTM cells for sequence progression along with the dense output layer used for classifications. An input matrix comprising 256×300 dimensions (256 words each represented by 300 embeddings) enables the LSTM layer to create a sequence of hidden states that flow into a dense processing system for classification outcome production.

3.6 Performance Metrics

The purpose of this study is to assess several sentiment analysis models, Multiple indicators used as performance metrics serve to evaluate the system. The metrics provide a complete assessment of how well the model performs in its sentiment classification of text documents into positive, negative, or neutral categories. A confusion matrix appears below to determine how accurately the classification model detects misidentified sentiments. The evaluation happens through sentiment label comparison between actual and predicted results, divided into four fundamental categories: TP and TN and FP, and FN. Here are brief definitions for the metrics utilized for evaluation:

1) Accuracy

Accuracy represents the relationship between correctly forecasted observations compared to the comprehensive observation count. The accuracy ratio demonstrates how well the classification model functions to detect genuine, along with fraudulent news content. The defined Equation (10) is as follows:

$$Accuracy = \frac{TP+TN}{TP+Fp+TN+FN} \quad (10)$$

2) Precision:

The ratio of correct positive predictions to total positive result forecasts is known as precision. Precise measurement serves both to verify fake news classification accuracy and guard cybersecurity systems against unnecessary false alarms according to the described mathematical basis in Equation (11).

$$Precision = \frac{TP}{TP+FP} \quad (11)$$

3) Recall

Also known as sensitivity or TP rate, recall is the proportion of correctly predicted positive observations to all actual positives. In fake news detection, it indicates how effectively the model identifies fake instances. Recall is expressed in Equation (12):

$$Recall = \frac{TP}{TP+FN} \quad (12)$$

4) F1-score

The F1-score provides a balance between recall and accuracy by functioning as the harmonic mean of the two, particularly in cases when the dataset is unbalanced, as is often the case in cybersecurity-related fake news detection, the F1-Score is considered among other evaluation metrics defined as Equation (13):

$$F1 - Score = 2\frac{(Precision*Recall)}{Precision + Reall} \quad (13)$$

5) Loss

To evaluate the effectiveness of their fake news detection model, to utilize appropriate loss functions and performance metrics that quantify the discrepancy between the predicted labels and the actual ones. The optimization of the model is guided during training by the loss function, ensuring convergence towards minimal error. For binary classification, the Loss is employed, defined as equation (14):

$$\mathcal{L}_{BCE} = -\frac{1}{N}\sum_{i=1}^{N}[y.\log(y_i) + (1 - y_i).\log(1 - \hat{y}_i)] \quad (14)$$

where: N is the total number of samples, y i $\in$ {0,1} is the true label for the i^{th} instance, $y \wedge i \in [0, 1]$ is the predicted probability of being a fake news item.

This loss penalizes the model more heavily when it makes confident but incorrect predictions, thus promoting accurate probabilistic outputs.

4. Result Analysis And Discussion

This section provides the findings and evaluation of the performed research. All experimental procedures were carried out on a machine includes 16GB of RAM and an Intel® Core™ i7 CPU, operating on Windows 10. The sentiment analysis and fake news detection models were developed using Python, leveraging key libraries including Scikit-learn, NumPy, Pandas, and Matplotlib for implementation and analysis. The proposed LSTM model is compared with XGBoost, and CNN, as shown in Table III. LSTM proves superior to all alternative algorithms for identifying false news stories using sentiment analysis, as shown in Table II:

TABLE II. RESULTS OF LSTM MODEL PERFORMANCE ON THE FAKE NEWS DATASET.

Measures	LSTM
Accuracy	95.1
Precision	94.4
Recall	95.3
F1-score	94.2

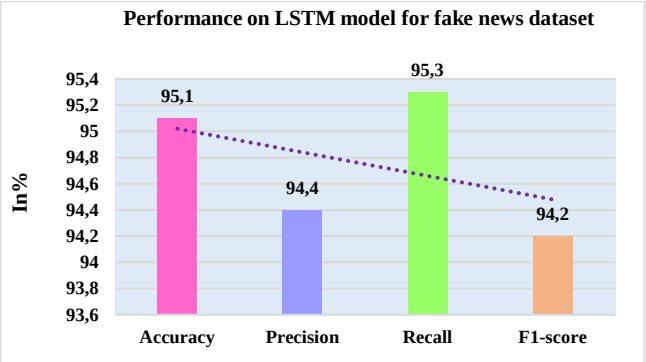


Fig. 5. Bar Graph for LSTM Model Performance

A LSTM model demonstrates its evaluation criteria performance through Table II alongside Figure 5. The model achieves a high accuracy level of 95.1% to show robust performance results. With a precision of 94.4%, the model demonstrates its capacity to detect positive examples. In addition to 95.3% recall, it demonstrates its effectiveness at finding all relevant positive cases. The F1-score of 94.2% represents an optimal balance between precision and recall attributes because the model shows dependable results across all aspects of predictions.

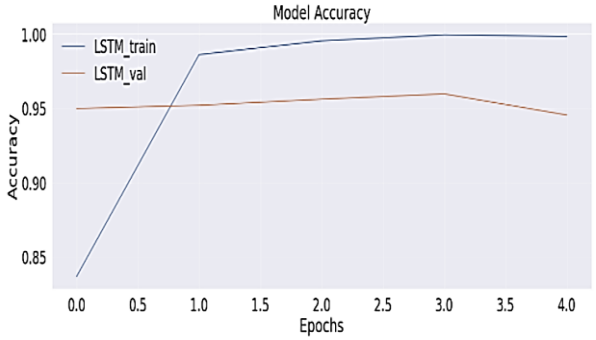


Fig. 6. Accuracy curve of LSTM Model

Figure 6 shows the accuracy of the LSTM model during its 5-epoch training process. The training accuracy increases rapidly, reaching nearly 99% by the second epoch and remaining stable, indicating the model is successfully assimilating the training data. Validation accuracy starts around 95%, improves slightly until the third epoch, and then declines in the final epoch. This pattern, coupled with the high training accuracy, suggests the model may be overfitting, as it shows reduced efficiency when applied to previously unknown validation data, even while training set results were exceptional.

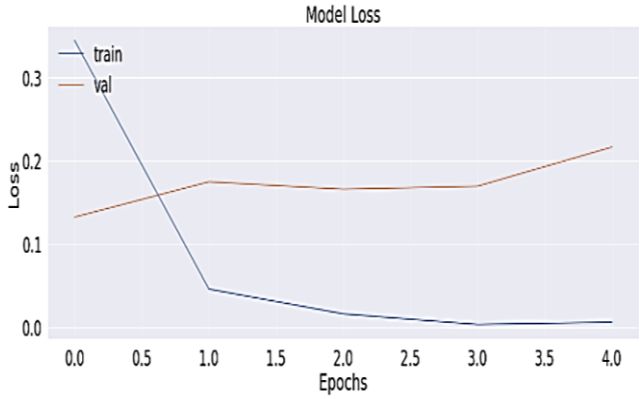


Fig. 7. Loss curve of LSTM Model

Figure 7 shows the training and validation losses for the LSTM model throughout five epochs. The training loss decreases sharply, reaching near-zero by the second epoch and remaining low, indicating the model fits the training data well. In contrast, the validation loss initially rises slightly, then stays relatively flat before increasing again in the final epoch. This divergence between the model may be overfitting if it performs well on training data but starts to lose generalization to fresh data, as shown by training and validation loss.

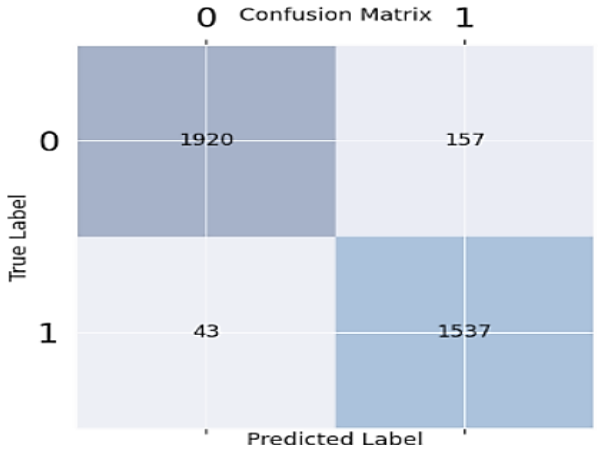


Fig. 8. Confusion Matrix of LSTM Model

The confusion matrix derived from a binary classification model is shown in Figure 8, where the negative class is represented by class "0" and the positive class by class "1". The model accurately classified 1920 true negatives and 1537 true positives, while 43 positive examples were incorrectly categorized as negative (FN) and 157 negative instances as positive (FP). The confusion matrix demonstrates strong overall performance, suggesting high sensitivity (recall) and specificity, with a relatively low number of misclassifications, thereby validating the model's effectiveness in distinguishing between the two classes.

5.1 Comparative Analysis and Discussion

The suggested LSTM model is compared in this section with existing models CNN [19] and XGBoost [20] evaluated on the false news dataset. The comparative performance of these models is shown in Table III.

TABLE III. COMPARATIVE RESULT OF MODEL PERFORMANCE ON THE FAKE NEWS DATASET USING ML AND DL MODELS

Models	Accuracy	Precision	Recall	F1-score
LSTM	95.1	94.4	95.3	94.2
CNN[19]	89	90	88	89
XGBoost[20]	83.2	83.6	83.2	82.9

The comparative analysis, as presented in Table III, highlights that The LSTM model performed best while processing sequential textual data, achieving the maximum 94.2% F1-score, 95.1% accuracy, 94.4% precision, and 95.3% recall. Having an 89% F1-score, 90% precision, 88% recall, and 89% correctness, the CNN model came in second, showing modest efficacy. In contrast, the XGBoost model showed the lowest performance, achieving an F1-score of 82.9%, recall of 83.2%, accuracy of 83.2%, and precision of 83.6%, indicating its relative shortcomings in identifying the intricate patterns needed for cybersecurity false news detection.

The effectiveness of LSTM models originates from their excel at processing sequential information within text data to

improve performance measurements, such as achieving 95.1% accuracy and 94.4% precision, together with 95.3% recall and 94.2% F1-score, demonstrating clear superiority over 89% accuracy for CNN and 83.2% accuracy for XGBoost. LSTM's gated architecture maintains updated information records through which it detects delicate linguistic patterns and sentiment indicators that other convolution-based models or tree structure models cannot recognize which resulting in better fake news detection reliability.

5. Conclusion And Future Direction

The ability to detect and identify false information quickly as well as accurately has become essential because digital media and social networks rapidly spread news in their present day. The negative consequences of fake news on public discourse and institutional stability, and social trust elements require effective detection solutions to combat the issue. The results of this research show that traditional machine learning methods work adequately by using LSTM deep learning networks, which demonstrate outperforming capabilities for detecting fake news statements. The LSTM model delivered an exceptional performance with 95.1% accuracy, along with 94.4% precision and 95.3% recall, along 94.2% F1-score. Research metrics confirm that the model identifies fake news better than traditional systems at a level where accuracy reaches 95.1%. LSTM's strength lies in its capability to understand long-term dependencies and context within text, allowing it to capture subtle semantic and syntactic cues that might otherwise be overlooked.

The model's expansion to multilingual datasets will be the main focus of future research, integrating streams of data in real time from social media sites, and enhancing model explain ability through attention mechanisms and visualization techniques. Additionally, further research will explore hybrid models combining LSTM with transformer-based architectures like BERT to improve performance and adaptability in dynamic online environments.

References

[1]. T. Saikh, A. Anand, A. Ekbal, and P. Bhattacharyya, "A Novel Approach Towards Fake News Detection: Deep Learning Augmented with Textual Entailment Features," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019. doi: 10.1007/978-3-030-23281-8_30.

[2]. M. T. Khan, M. Durrani, A. Ali, I. Inayat, S. Khalid, and K. H. Khan, "Sentiment analysis and the complex natural language," *Complex Adaptive Systems Modeling*. 2016. doi: 10.1186/s40294-016-0016-9.

[3]. F. A. Ozbay and B. Alatas, "A novel approach for detection of fake news on social media using metaheuristic optimization algorithms," *Elektron. ir Elektrotechnika*, 2019, doi: 10.5755/j01.eie.25.4.23972.

[4]. S. Paul, J. I. Joy, S. Sarker, A. A. H. Shakib, S. Ahmed, and A. K. Das, "Fake News Detection in Social Media using Blockchain," in *2019 7th International Conference on Smart Computing and Communications, ICSCC 2019*, 2019. doi: 10.1109/ICSCC.2019.8843597.

[5]. B. V. P. Kumar, G. Pramod, L. Mohan, and A. V. R. Reddy, "Classifying Fake News Articles Using Natural Language Processing to Identify in-Article Attribution As A Supervised Learning Estimator," *Turkish J. Comput. Math. Educ.*, vol. 10, no. 3, pp. 1243–1246, Dec. 2019, doi: 10.61841/turcomat.v10i3.14460.

[6]. D. D. Rao, "Multimedia based intelligent content networking for future internet," *EMS 2009 - UKSim 3rd Eur. Model. Symp. Comput. Model. Simul.*, pp. 55–59, 2009, doi: 10.1109/EMS.2009.108.

[7]. R. Barua, R. Maity, D. Minj, T. Barua, and A. K. Layek, "F-NAD: An Application for Fake News Article Detection using Machine Learning Techniques," in *2019 IEEE Bombay Section Signature Conference, IBSSC 2019*, 2019. doi: 10.1109/IBSSC47189.2019.8973059.

[8]. N. Deligiannis, T. Do Huu, D. M. Nguyen, and X. Luo, "Deep Learning for Geolocating Social Media Users and Detecting Fake News," *NATO Work.*, 2018.

[9]. R. K. Kaliyar, A. Goswami, and P. Narang, "Multiclass Fake News Detection using Ensemble Machine Learning," in *Proceedings of the 2019 IEEE 9th International Conference on Advanced Computing, IACC 2019*, 2019. doi: 10.1109/IACC48062.2019.8971579.

[10]. S. Bauskar, V. Badole, P. Jain, and M. Chawla, "Natural Language Processing based Hybrid Model for Detecting Fake News Using Content-Based Features and Social Features," *Int. J. Inf. Eng. Electron. Bus.*, 2019, doi: 10.5815/ijieeb.2019.04.01.

[11]. A. Lakshmanarao, Y. Swathi, and T. Srinivasa Ravi Kiran, "An effecient fake news detection system using machine learning," *Int. J. Innov. Technol. Explor. Eng.*, 2019, doi: 10.35940/ijitee.J9453.0881019.

[12]. V. Kolluri, "A Pioneering Approach To Forensic Insights: Utilization AI for Cybersecurity Incident Investigations," *Int. J. Res. Anal. Rev.*, vol. 3, no. 3, 2016.

[13]. P. Karthika, R. Murugeswari, and R. Manoranjithem, "Sentiment Analysis of Social Media Network Using Random Forest Algorithm," in *IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing, INCOS 2019*, 2019. doi: 10.1109/INCOS45849.2019.8951367.

[14]. M. Yadav and V. Bhojane, "Semi-Supervised Mix-Hindi Sentiment Analysis using Neural Network," in *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, IEEE, Jan. 2019, pp. 309–314. doi: 10.1109/CONFLUENCE.2019.8776943.

[15]. E. Qawasmeh, M. Tawalbeh, and M. Abdullah, "Automatic Identification of Fake News Using Deep Learning," in *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)*, IEEE, Oct. 2019, pp. 383–388. doi: 10.1109/SNAMS.2019.8931873.

[16]. R. K. Kaliyar, A. Goswami, and P. Narang, "Multiclass Fake News Detection using Ensemble Machine Learning," in *2019 IEEE 9th International Conference on Advanced Computing (IACC)*, 2019, pp. 103–107. doi: 10.1109/IACC48062.2019.8971579.

[17]. D. Aksu and M. Ali Aydin, "Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and Support Vector Machine Algorithms," in *2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)*, IEEE, Dec. 2018, pp. 77–80. doi: 10.1109/IBIGDELFT.2018.8625370.

[18]. C.-J. Huang and P.-H. Kuo, "A Deep CNN-LSTM Model for Particulate Matter (PM2.5) Forecasting in Smart Cities," *Sensors*, vol. 18, no. 7, p. 2220, Jul. 2018, doi: 10.3390/s18072220.

[19]. B. M. Amine, A. Drif, and S. Giordano, "Merging deep learning model for fake news detection," in *2019 International Conference on Advanced Electrical Engineering, ICAEE 2019*, 2019. doi: 10.1109/ICAEE47123.2019.9015097.

[20]. J. Lin, G. Tremblay-Taylor, G. Mou, D. You, and K. Lee, "Detecting Fake News Articles," in *Proceedings - 2019 IEEE International Conference on Big Data, Big Data 2019*, 2019. doi: 10.1109/BigData47090.2019.9005980.

[21]. R. Swamidurai, U. Kannan, A. Raglin, and L. Scott, "Smart City Internet of Things Reasoning System for Emergency Responders," in *Conference Proceedings - IEEE SOUTHEASTCON*, 2019. doi: 10.1109/SoutheastCon42311.2019.9020580.

[22]. Bodepudi, V., & Chinta, P. C. R. (2024). Enhancing Financial Predictions Based on Bitcoin Prices using Big Data and Deep Learning Approach. *Available at SSRN 5112132*.

[23]. Chinta, P. C. R. (2023). The Art of Business Analysis in Information Management Projects: Best Practices and Insights. *DOI*, *10*.

[24]. Chinta, P. C. R., & Katnapally, N. (2021). Neural Network-Based Risk Assessment for Cybersecurity in Big Data-Oriented ERP Infrastructures. *Neural Network-Based Risk Assessment for Cybersecurity in Big Data-Oriented ERP Infrastructures*.

[25]. Katnapally, N., Chinta, P. C. R., Routhu, K. K., Velaga, V., Bodepudi, V., & Karaka, L. M. (2021). Leveraging Big Data Analytics and Machine Learning Techniques for Sentiment Analysis of Amazon Product Reviews in Business Insights. *American Journal of Computing and Engineering*, *4*(2), 35-51.

[26]. Chinta, P. C. R., Moore, C. S., Karaka, L. M., Sakuru, M., Bodepudi, V., & Maka, S. R. (2025). Building an Intelligent Phishing Email Detection System Using Machine Learning and Feature Engineering. *European Journal of Applied Science, Engineering and Technology*, *3*(2), 41-54.

[27]. Moore, C. (2024). Enhancing Network Security With Artificial Intelligence Based Traffic Anomaly Detection In Big Data Systems. Available at SSRN 5103209.

[28]. Chinta, P. C. R., Moore, C. S., Karaka, L. M., Sakuru, M., & Bodepudi, V. (2025). Predictive Analytics for Disease Diagnosis: A Study on Healthcare Data with Machine Learning Algorithms and Big Data. *J Cancer Sci*, *10*(1), 1.

[29]. Chinta, P. C. R., Jha, K. M., Velaga, V., Moore, C., Routhu, K., & SADARAM, G. (2024). Harnessing Big Data and AI-Driven ERP Systems to Enhance Cybersecurity Resilience in Real-Time Threat Environments. *Available at SSRN 5151788*.

[30]. Chinta, P. C. R. (2023). Leveraging Machine Learning Techniques for Predictive Analysis in Merger and Acquisition (M&A). *Journal of Artificial Intelligence and Big Data*, *3*(1), 10-31586.

[31]. Chinta, P. C. R. (2022). Enhancing Supply Chain Efficiency and Performance Through ERP Optimisation Strategies. *Journal of Artificial Intelligence & Cloud Computing*, *1*(4), 10-47363.

[32]. Chinta, P. C. R., & Karaka, L. M. AGENTIC AI AND REINFORCEMENT LEARNING: TOWARDS MORE AUTONOMOUS AND ADAPTIVE AI SYSTEMS.

[33]. Sadaram, G., Karaka, L. M., Maka, S. R., Sakuru, M., Boppana, S. B., & Katnapally, N. (2024). AI-Powered Cyber Threat Detection: Leveraging Machine Learning for Real-Time Anomaly Identification and Threat Mitigation. MSW Management Journal, 34(2), 788-803.

[34]. Krishna Madhav, J., Varun, B., Niharika, K., Srinivasa Rao, M., & Laxmana Murthy, K. (2023). Optimising Sales Forecasts in ERP Systems Using Machine Learning and Predictive Analytics. *J Contemp Edu Theo Artific Intel: JCETAI-104*.

[35]. Sadaram, G., Sakuru, M., Karaka, L. M., Reddy, M. S., Bodepudi, V., Boppana, S. B., & Maka, S. R. (2022). Internet of Things (IoT) Cybersecurity Enhancement through Artificial Intelligence: A Study on Intrusion Detection Systems. *Universal Library of Engineering Technology*, (2022).

[36]. Jha, K. M., Velaga, V., Routhu, K. K., Sadaram, G., & Boppana, S. B. (2025). Evaluating the Effectiveness of Machine Learning for Heart

Disease Prediction in Healthcare Sector. *J Cardiobiol*, *9*(1), 1.

[37]. Maka, S. R. (2023). Understanding the Fundamentals of Digital Transformation in Financial Services: Drivers and Strategic Insights. *Available at SSRN 5116707*.

[38]. Karaka, L. M. (2021). Optimising Product Enhancements Strategic Approaches to Managing Complexity. *Available at SSRN 5147875*.

[39]. KishanKumar Routhu, A. D. P. Risk Management in Enterprise Merger and Acquisition (M&A): A Review of Approaches and Best Practices.

[40]. Routhu, KishanKumar & Katnapally, Niharika & Sakuru, Manikanth. (2023). Machine Learning for Cyber Defense: A Comparative Analysis of Supervised and Unsupervised Learning Approaches. Journal for ReAttach Therapy and Developmental Diversities. 6. 10.53555/jrtdd.v6i10s(2).3481.

[41]. Kalla, D., Smith, N., Samaah, F., & Polimetla, K. (2022). Enhancing Early Diagnosis: Machine Learning Applications in Diabetes Prediction. *Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-205. DOI: doi. org/10.47363/JAICC/2022 (1)*, *191*, 2-7.

[42]. Chinta, Purna Chandra Rao & Moore, Chethan Sriharsha. (2023). Cloud-Based AI and Big Data Analytics for Real-Time Business Decision-Making. 36. 96-123. 10.47363/JAICC/2023.

[43]. Kuraku, D. S., & Kalla, D. (2023). Phishing Website URL's Detection Using NLP and Machine Learning Techniques. *Journal on Artificial Intelligence-Tech Science*.

[44]. Krishna Madhav, J., Varun, B., Niharika, K., Srinivasa Rao, M., & Laxmana Murthy, K. (2023). Optimising Sales Forecasts in ERP Systems Using Machine Learning and Predictive Analytics. *J Contemp Edu Theo Artific Intel: JCETAI-104*.

[45]. Jha, K. M., Velaga, V., Routhu, K., Sadaram, G., Boppana, S. B., & Katnapally, N. (2025). Transforming Supply Chain Performance Based on Electronic Data Interchange (EDI) Integration: A Detailed Analysis. *European Journal of Applied Science, Engineering and Technology*, *3*(2), 25-40.

[46]. Kuraku, D. S., & Kalla, D. (2023). Phishing Website URL's Detection Using NLP and Machine Learning Techniques. *Journal on Artificial Intelligence-Tech Science*.

[47]. Jha, K. M., Velaga, V., Routhu, K. K., Sadaram, G., & Boppana, S. B. (2025). Evaluating the Effectiveness of Machine Learning for Heart Disease Prediction in Healthcare Sector. *J Cardiobiol*, *9*(1), 1.

[48]. KishanKumar Routhu, A. D. P. Risk Management in Enterprise Merger and Acquisition (M&A): A Review of Approaches and Best Practices.

[49]. Kalla, D., Mohammed, A. S., Boddapati, V. N., Jiwani, N., & Kiruthiga, T. (2024, November). Investigating the Impact of Heuristic Algorithms on Cyberthreat Detection. In *2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)* (Vol. 1, pp. 450-455). IEEE.

[50]. Bodepudi, V. (2023). Understanding the Fundamentals of Digital Transformation in Financial Services: Drivers and Strategic Insights. *Journal of Artificial Intelligence and Big Data*, *3*(1), 10-31586.

[51]. Kalla, D., Smith, N., & Samaah, F. (2025). Deep Learning-Based Sentiment Analysis: Enhancing IMDb Review Classification with LSTM Models. *Available at SSRN 5103558*.

[52]. Jha, K. M., Bodepudi, V., Boppana, S. B., Katnapally, N., Maka, S. R., & Sakuru, M. Deep Learning-Enabled Big Data Analytics for Cybersecurity Threat Detection in ERP Ecosystems.

[53]. Kalla, D., Samaah, F., Kuraku, S., & Smith, N. (2023). Phishing detection implementation using databricks and artificial Intelligence. *International Journal of Computer Applications*, *185*(11), 1-11.

[54]. Boppana, S. B., Moore, C. S., Bodepudi, V., Jha, K. M., Maka, S. R., & Sadaram, G. AI And ML Applications In Big Data Analytics: Transforming ERP Security Models For Modern Enterprises.

[55]. Sreeramulu, M. D., Mohammed, A. S., Kalla, D., Boddapati, N., & Natarajan, Y. (2024, September). AI-driven Dynamic Workload Balancing for Real-time Applications on Cloud Infrastructure. In *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)* (Vol. 7, pp. 1660-1665). IEEE.

[56]. Kalla, D., & Samaah, F. (2023). Exploring Artificial Intelligence And Data-Driven Techniques For Anomaly Detection In Cloud Security. *Available at SSRN 5045491*.

[57]. Kalla, D., Smith, N., & Samaah, F. (2023). Satellite Image Processing Using Azure Databricks and Residual Neural Network.