Journal of Intelligent Systems and Internet of Things
Vol. 15, No. 02, PP. 104-120, 2025
DOI: https://doi.org/10.54216/JISIoT.150208

Enhancing E-commerce Security through Fake News Detection Using Natural Language Processing and Advanced Feature Engineering Technique

Lama Sameer Khoshaim[1,*]
[1]Assistant Professor, Department of e-Commerce, College of Administrative and Financial Sciences, Saudi Electronic University, Jeddah, Saudi Arabia
Email: l.khoshaim@seu.edu.sa

Abstract

E-commerce has simplified customers' lives and offered a range of items, but it has also made them vulnerable to frauds. Fake news on e-commerce platforms threatens trust, brand image, and economic stability. Researchers have shown that contemporary Natural Language Processing (NLP) and machine learning can stop bogus news. However, e-commerce companies still struggle to distinguish phony news from real information. Fast knowledge diffusion can cause financial loss, reputation damage, and customer distrust. Thus, e-commerce false news identification requires robust and trustworthy methods. This investigation will successfully recognize and discriminate fake news. High Feature Extraction uses Word2vec and Term Frequency-Inverse Document Frequency (TF-IDF) to extract features. The optimum feature subset is determined via feature selection utilizing the least absolute shrinkage and selector operator (LASSO). The study involves four phases: Extraction, selection, classification, and data processing are the four steps. To remove raw data, data preparation utilizes stemming, lemmatization, and stop word removal. The suggested method averages model outputs to reduce overfitting and improve prediction stability. DIstilBERT with multi-stacked LSTM is tested on WELFake and ranked by F1 score, sensitivity, accuracy, and specificity. The multi-stacked LSTM distiller has 99.77% accuracy, far greater than the others do. We can use it to detect bogus news. It boosts customer confidence and Internet commerce legitimacy by improving accuracy and consistency.

Received: September 25, 2024 Revised: November 27, 2024 Accepted: January 17, 2025

Keywords: E-Commerce; High Feature Extraction (HFE); DistilBERT; Multi-stacked LSTM; Least Absolute Shrinkage and Selection Operator (LASSO)

1. Introduction

Over the past few years, e-commerce has rapidly evolved into a new way through which customers engage with sellers and make their purchases [1]. This digital revolution has had several advantages such as; ease, variety and price. However, the advancement of e-commerce platforms has also brought about new problems, especially for the problem of information accuracy and security [2]. Another challenge attributed to e-commerce companies in the current world is the issue of fake news and other fraud-related activities. The fake news in the e-commerce context can be in the form of fake reviews, fake and misleading advertisements, and fake descriptions of the products. Such fraudulent activities are not only detrimental to consumers and their trust but also present considerable financial risks to consumers and businesses [3]. It causes wrong buying decisions, monetary losses, and negative impacts on the image of the online vendors. Thus, the identification and prevention of fake news has emerged as a significant challenge for e-commerce companies that seek to guarantee consumers' trust and protect them from frauds [4].

It is almost indispensable nowadays to point out the necessity of identifying false news in the digital era, which is the time of fast information discountable on internet for ordinary users. 'Fake news' is one of the critical challenges nowadays because it is the news that are deliberately created to fool people and present the false information as real news [5]. It itself can make the rules, forming public opinions, stirring up conflict, and undermining the trust

in the institutions and the mass media. Another example is fake news, which can affect election results, promote violence and even risk a person's life through broadcasting incorrect and misleading information that can be related to the crisis, the state of health or emergency [6]. In this case, the quickness and accuracy of identifying and combating false news stories is the essential element that must be provided to ensure the safety of information systems and to base the decision-making on data [7]. This procedure of detecting fake news additionally prevents the public from being misled but also the principles of truth, accuracy, and accountability in media and journalism are maintained as well [8].

The fake news scourge is extreme in the recent battles like the one on the Russian invasion of Ukraine [9]. In these cases, fighting and information competition are the dominant strategies used by both sides and they mostly participate through strategic communication as a means to define narratives. Besides, the perpetrators of this information havoc are not only confined in Russia but they also use false news and misinformation to dupe the public mind, and in order to gain strategic advantage. Sometimes it happens that movie makers fail to show all aspects of the conflict, which can lead to wrong interpretation of the conflict, which will hinder peace process and increases tension. In addition, the threat of the dissemination of untrustworthy information in the conflict areas is a very dangerous one, because it may lead to violence and endanger the process of delivery of humanitarian aid [10].

The key goal of this paper is to come up with an answer to the situation of the growing fake news problem, which has started to become a significant problem for global trust and society. The internet is the main factor involved with the spreading of rumours and misinformation nowadays; hence, the articles that follow suit are proved inaccurate [11]. The absence of the correct user verification is the main factor, which intensifies this issue and leads to the spread of false news on the large-scale media platforms, [12]. To counteract this issue efficiently, there is an urgent need for advanced methods that can reliably spot false news.

This research aims to propose and explore a new model for improving fake news recognition capability in digital media. The primary emphasis of the study will be on the use of a variety of methods including TF-IDF and the word2vec algorithm, under the umbrella of HFE, to extract relevant features that will be of help in the accurate identification the counterfeit news. It is therefore necessary to conduct research that aims to enhance the feature selection process by applying the LASSO, which will help in identifying the most discriminative feature subset. The study unfolds through four key stages: data pre-processing, feature selection, feature extraction, and classification as the main techniques and the entire goal of the fake news detector will be to improve its efficiency and accuracy. Additionally, the method that is proposed can diminish the risk of overfitting and reinforce the accuracy of the forecast with the help of the output aggregation from multiple models. The assessment of the DistilBERT models with the multi-stacking LSTM method on the WELFake dataset is carried out to measure its performance regarding specificity, sensitivity, accuracy, and F1 score. The evaluation of this approach employing the WELFake dataset shows that it far outperforms its counterparts, with an accuracy of 99.82% that show it could function as an instrument of combating fake news, and defence of assuring the authenticity of information. The main contributions of this study are as follows:

- The study enhances the feature extraction by using the combination of Word2vec and TF-IDF. Therefore, the text model can discover the most significant features for text data.
- LASSO is applied to select the most pertinent features by the model, thus improving the accuracy and making it simpler.
- Stemming, lemmas, and stop words are employed to ensure the data is prepared in a clean and unified format prior to entering into the modelling process.
- The approach, which is a combination of LSTM network with the DistilBERT model, is introduced in order to reach perfect accuracy.
- The model gives an amazing accuracy of 99.77% on the WELFake data set and employs the results obtained from several models to minimize overfitting and improve stability of the prediction.

The remainder of the paper is organized as follows: The Literature Review, which highlights research gaps and limitations in the current fake news detection techniques, is presented in Section 2. A description of the dataset, pre-processing procedures, feature extraction using Word2vec and TF-IDF, feature selection using LASSO, and the hybrid DistilBERT with multi-stacked LSTM model are all covered in Section 3's Materials & Methods section. The experimental results of the proposed approach are shown in Section 4. Section 5 provides a discussion of results with interpretation alongside an examination of model advantages and overfitting prevention strategies and its implications for natural language processing and false news detection. Section 6 presents a summary of the paper's main contributions while emphasizing model effectiveness and potential research directions.

2. Literature review

Research into fake news detection has emerged as essential because misinformation spreads rapidly across multiple domains including e-commerce. This review examines the essential developments in fake news detection by analysing methods alongside NLP and machine learning progress, which affect e-commerce platforms.

The increasing number of online security threats in e-commerce has prompted researchers to study phishing attacks and banking frauds and other deceptive practices. The research by Pinjarkar et al. (2024) investigates standard frauds involving ATM skimming and bogus loan offers to emphasize the requirement for better online safety practices. Research shows that cybercriminals employ phishing methods to obtain personal data while organizations face continuous difficulties protecting sensitive information from developing threats. Keshri et al. (2020) analyse how rumours damage e-commerce consumer trust by revealing how false information erodes platform confidence.

Research has made advanced mathematical modelling and machine learning applications central to e-commerce security investigations. Yadav and Keshri (2024) established an epidemic mathematical modelling framework, which integrates neural networks to defend e-commerce systems. The method uncovers hidden fake news propagation patterns between consumer actions while showing the importance of complex models for combating emerging security threats. E-RLSTM technology integration enhances fake news detection accuracy beyond traditional approaches while facing ongoing challenges to adapt to constantly changing fake news propagation patterns.

The e-commerce industry encounters critical security threats from malware attacks and ransomware incidents and phishing threats and SQL injection breaches that platform operators must address. Dakov and Malinova (2021) present a detailed assessment of security threats and protective measures by combining encryption with secure payment systems. The expanding e-commerce landscape creates more security weaknesses, which demand ongoing security monitoring from providers and consumers. Desamsetti (2021) demonstrates how criminal hacker's exploitation of both technological systems and human elements puts e-commerce security at risk.

Studies about risk management and security practice implementation focus on the critical need for permanent security measures that train personnel, update systems, and enforce robust policies. Gupta (2024) provides encryption and secure payment gateway mitigation strategies alongside Harshavardan and PadmaShani (2023) who focus on secure practices to stop cyber-attacks in e-commerce sites. E-commerce businesses face an ongoing cybersecurity challenge because cyber threats continually evolve in their complexity. Research acknowledges that risk management strategies remain incomplete while attackers constantly develop new sophisticated methods.

A. Research Gaps

Multiple essential gaps exist in the current research about e-commerce security threats that occur online. Research has thoroughly analysed traditional threats like phishing and banking frauds and malware but emerging threats from advanced social engineering and AI-powered attacks receive insufficient attention because they are becoming more complex. Advanced mathematical models along with machine learning methods demonstrate potential for threat detection yet their practical implementation and operational complexity remains understudied. Longitudinal data on the long-term effectiveness of current security measures is sparse, leaving a gap in understanding the evolving nature of threats and the sustainability of existing solutions. Furthermore, there is insufficient research on the human factors contributing to security breaches, such as employee training and policy enforcement, which are critical in the fight against cybercrime. Lastly, many studies lack generalizability across diverse e-commerce contexts, leaving a need for more scalable and adaptable security models that can address the varied needs of e-commerce platforms globally. Addressing these gaps will require a more comprehensive, long-term, and adaptable approach to e-commerce security. The summary of literature review is presented in Table 1.

Table 1: summary of literature review

Reference	Method	Findings	Limitations
Pinjarkar et al. (2024) [13]	Examination of phishing, banking frauds, and e-commerce deceptions.	Cybercriminals use phishing to steal personal information.	Limited focus on specific types of online frauds.
Yadav and Keshri (2024) [14]	Epidemic mathematical modeling with neural networks.	E-RLSTM technique outperforms others in fake news propagation analysis.	Complexity of the epidemic modeling approach.

Keshri et al. (2020) [15]	Numerical simulations to evaluate rumor spreading in e-commerce.	Rumors negatively affect consumer trust in e-commerce.	Limited exploration of the broader effects on consumer behavior.
Dakov and Malinova (2021) [16]	Survey of e-commerce security threats and solutions.	Encryption firewalls, and secure payment systems are effective at mitigating threats.	Focus on existing security tools without exploring emerging threats.
Desamsetti (2021) [17]	Analysis of cybersecurity threats such as social engineering, malware, and DDoS attacks.	Emphasized the importance of technology, staff training, and strong policies to mitigate threats.	Constantly evolving threats make it difficult to achieve permanent security.
Gupta (2024) [18]	Survey of cybersecurity mitigation strategies for e-commerce.	Strategies like encryption and secure payment gateways help mitigate threats in e-commerce.	Limited to well-known threats and lacks focus on new security issues.
Harshavardan and PadmaShani (2023) [19]	Discussion of secure practices to prevent cyber-attacks in e-commerce.	Highlights the necessity of secure practices like phishing protection and malware mitigation.	Focuses on practical solutions without addressing scalability.
Li et al. (2021) [20]	Fake click detection techniques in e-commerce recommendation systems.	Proposed techniques for detecting large-scale fake clicks effectively.	Limited studies on false click behavior in e-commerce systems.
Cidon et al. (2019) [21]	Supervised learning to detect business email compromise.	High precision detection of business email compromise through email header and body analysis.	Requires labeling a vast number of emails, which is labor-intensive.
Liu et al. (2022) [22]	Quantification of e-risk probability using Logit and Probit models.	Models quantify e-threat probabilities to help mitigate financial losses from security breaches.	May not account for complex or evolving cybersecurity risks.
Mitra et al. (2022) [23]	Survey of social engineering, denial of service, and malware threats.	Identified key cybersecurity threats such as malware and data breaches, and suggested mitigation measures.	Further research needed on other aspects of cybersecurity threats.
Jamra et al. (2020) [24]	Analysis of cybersecurity challenges in e-commerce business.	Discusses mitigation strategies such as encryption and employee training to address cybersecurity threats.	Erosion of confidence in digital security from major data leaks.
Alotaibi and Mehmood (2022) [25]	Systematic review of e-commerce security issues and solutions.	Provides secure shopping guidelines and solutions to tackle e-commerce security issues.	Limited to existing guidelines and security technologies.

3. Materials and Methods

The DistilBERT-stacked-LSTM method for fake news recognition follows the processes shown in Figure 1 through a sequential order. The process starts with dataset acquisition followed immediately by data cleaning and formatting. The prepared data leads to the creation of hybrid features. A subset of relevant features is selected via LASSO feature selection before moving onto classification. SEC algorithm performs classification on the selected features. The DistilBERT LSTM model works to reduce overfitting so the method achieves better generalization results. The aggregation of results using a MLP improves prediction stability within the system. This systematic methodology demonstrates the complete procedure for detecting fake news through its implementation of DistilBERT-LSTM methods. The following sub-sections provide a detailed explanation of the proposed methodology.

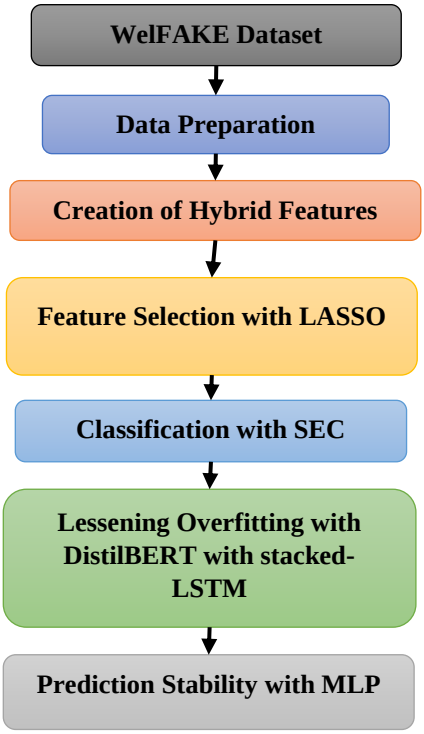

Figure 1. Block diagram of the proposed method

A. Data Acquisition

The WELFake dataset serves as the primary source for this study because it includes labeled real and fake news articles specifically created for detecting e-commerce fake news. The dataset provides wide-ranging text material that enables successful machine learning model training and assessment. A preprocessing pipeline of stemming with lemmatization and stop-word elimination becomes part of the data preparation process, which aims to reduce extraneous information that directs model attention toward essential features.

The WELFake dataset contains 72,134 news articles split into 35,028 real news articles and 37,106 fake news articles. A new dataset emerged from combining four established news datasets including Kaggle and McIntire and Reuters and BuzzFeed Political. The integration of these diverse sources serves two primary purposes: first, to mitigate the risk of overfitting in machine learning classifiers by providing a more varied and representative dataset, and second, to enhance the robustness and accuracy of machine learning training through the availability of a larger corpus of textual data. The dataset is organized into four distinct columns. The first column, "Serial Number," provides a unique identifier for each entry, starting from 0. The second column, "Title," contains the headlines of the news articles, offering a brief summary of their content. The third column, "Text," provides the full body of the news content, enabling deeper analysis of the linguistic and contextual features of the articles. The fourth column, "Label," categorizes the news articles, where a value of 0 represents fake news, and a value of 1 denotes real news. The dataset, available in CSV format, contains 78,098 entries. However, only 72,134 entries are actively utilized in the data frame for analysis and model training purposes, ensuring a clean and consistent structure for machine learning workflows. This dataset was published in the IEEE Transactions on Computational Social Systems (Volume and page details: pp. 1-13) and can be accessed via its DOI:10.1109/TCSS.2021.3068519.

It serves as a valuable resource for researchers and practitioners in the domain of fake news detection and computational social systems.

B. Data Pre-Processing

Using the following methods, the raw data from the WELFake dataset is pre-processed according to the following procedures:

- Stemming: Text characteristics are converted to root words using the Porter-Stemmer technique [41]. It generates the canonical form of an analogous word if it is unable to determine the underlying word.
- Lemmatization: This process converts the input words into a uniformly applicable canonical form [42].

Lastly, stop word elimination is used to eliminate stop words from the input, since their contribution is less than that of the remaining relevant data. Figure 2 displays the result that has been pre-processed. The data is handled under feature engineering to extract features once it has been pre-processed using the previously outlined methods.

```
RT joshjeje2 surprise find out jennif bamuturaki ceo uganda airline onli earn 20million rest
american airline purchase boom superson overturn aircraft http flight to america go
man punch face flight attend sentence http
jetblu rais offer again bid spirit airline travel weekli
RT  dailymonitor do not matter whether I go moon whether I did mdd matter do I have skill  and I do I can
plane debut 2029 ticket cost about $ 4,000 $ 5,000 fly from new york london three
americanair sign agreement with boomaero purchase 20  firm  overturn aircraft
swissport celebr 15 year cargohandl asiana airlin brusselsairport 2007 began program
icymi  more than 64000 employe intern airlin group iag consid one world  largest
brianmixologist joelssenyonyi ug_airlin jonahruhima eyaru_levi wadadamichael theotheguyher bandiva
```

Figure 2. Pre0processed Output

C. Feature Extraction

Finding the expressive characteristics in data for a successful categorization is known as feature engineering. At this point, the pre-processed input is subjected to a feature extraction method using a mix of TF-IDF and Word2vec. The steps involved in feature extraction are broken down as follows:

Term Frequency-Inverse Document Frequency (TF-IDF)

TF-IDF is a statistical measure that evaluates the importance of a word in a document relative to a collection (or corpus) of documents. It combines term frequency (how often a word appears in a document) with inverse document frequency (how unique the word is across the corpus). TF-IDF is employed to identify significant terms that contribute most to the classification task. By emphasizing rare yet informative words, TF-IDF ensures that the model focuses on distinctive features that help differentiate fake news from real news.

The TF-IDF characteristics that were retrieved from the sample are displayed in Figure 3.

```
'post': 7547, 'company': 2890, 'annoyed': 1587, 'weather': 10541, 'relate': 8071, 'flightd': 4371,
'incompetence': 5348, 'need2know': 6740, 'ill': 5276, 'able': 1263, 'reach': 7915, 'ind': 5372,
'today': 9707, 'stay': 9127, 'maf': 6247, 'fly': 4416, 'dfw': 3463, 'travel': 9797, 'gvgkhbx1rb':
4882, 'wth': 10769, 'honest': 5116, 'better': 2077, 'change': 2597, 'driving': 3722, 'home': 5111,
'plane': 7457, 'left': 5957, 'gave': 4646, 'lying': 6226, 'raising': 7880, 'voice': 10411,
'explanation': 4100, 'happened': 4930, '31cfhtk60r': 544, '1777': 247, 'waiting': 10461, '30': 519,
'minutes': 6505, 'rsw': 8369, 'weight': 10561, 'balance': 1944, 'clearance': 2749, 'come': 2849,
'let': 5975, 'leave': 5950, 'hold': 5095, '5am': 880, 'cancelled': 2459, 'make': 6268, 'huge': 5197,
'fee': 4235, 'window': 10642, 'airbus321seat14fproblems': 1427, 'zkoe6clgiu': 10892, 'yes':
10823, 'nvr': 6956, 'missed': 6532, 'coffeemaker': 2820, 'ft1892': 4569, 'couldn': 3083, 'father':
4206, 'be4': 2006, 'coma': 2842, 'yeah': 10812, 'tried': 9832, '10': 31, 'times': 9666, 'different':
3488, 'tickets': 9647, 'late': 5898, 'flightr': 4387, 'thnkx': 9611, 'bt': 2322, 'dont': 3662, 'help':
5020, 'need': 6739, 'way': 10526, 'charge': 2609, 'sux': 9350, 'neveragain': 6768, 'sharing': 8690,
'photos': 7397, 'round': 8350, 'applause': 1640, 'crews': 3151, 'appreciate': 1652, 'hard': 4943,
'work': 10702, 'changes': 2599, 'website': 10548, 'charged': 2610, '25': 428, 'dollars': 3650,
'phone': 7391, 'day': 3291, 'yesterday': 10826, '3x': 643, 'info': 5405, 'didnt': 3480, 'bought':
2229, 'went': 10573, 'amazing': 1518, 'best': 2066, 'kidding': 5789, 'incredible': 5366, 'wait':
10458, 'll': 6070, 'contain': 3010, 'roundtrip': 8351, 'london': 6120, 'delta': 3380, 'think': 9600,
'fyi': 4619, '1k': 306, 'just': 5721, 'lost': 6148, 'moneynotspentonunited': 6585, 'unfriendlyskies':
10123, 'gate': 4643, 'checkin': 2639, 'book': 2196, 'clients': 2761, 'believe': 2046, 'lack': 5857,
'dialing': 3470, 'callback': 2438, 'queue': 7839, 'states': 9119, 'playing': 7477, 'hunt': 5213,
'destinationdragons': 3440, 'admirals': 1359, 'club': 2784, 'clt': 2783, 'rude': 8377, 'ignorant':
5267, 'desk': 3430, 'staff': 9087, 'fallen': 4173, 'far': 4188, 'doug': 3681, 'parker': 7249, 'jal':
5593, 'cathay': 2530, 'pacific': 7200, 'online': 7057, 'yup': 10865, 'fault': 4208, 'ideal': 5247,
'sittin': 8811, 'hour': 5170, 'great': 4811, 'bougth': 2230, 'fligths': 4393, 'twice': 9906, 'refund':
8035, 'money': 6583, 'big': 2096, 'problem': 7673, 'tell': 9503, 'keepingit100': 5764, 'weaktea':
10536, 'thankful': 9546, 'orf': 7098, 'dca': 3300, 'ground': 4837, 'air': 1425, 'sick': 8765, 'kid':
5788, 'bag': 1928, 'telling': 9505, 'correct': 3064, 'tag': 9422, 'luggage': 6204, 'apparently': 1633,
'la': 5854, 'charlotte': 2617, 'ok': 7026, 'jtrexsocial': 5705, 'hours': 5174, 'safe': 8428, 'say': 8498,
'working': 10708, '435': 703, 'delayed': 3360, 'miss': 6531, 'connecting': 2975, '457': 743,
'alternate': 1502, 'thank': 9544, 'train': 9771, 'support': 9321, 'appropriate': 1658, 'decorum':
3333, 'consider': 2983, 'revisiting': 8248, 'terrible': 9519, 'provide': 7741, 'death': 3313,
```

Figure 3. Sample extracted features of TF-IDF

Word2vec

One well-liked sequence embedding technique that transforms natural language into a distributed vector representation is called Word2vec [44]. The contextual word-to-word associations throughout the multidimensional space are extracted using this Word2vec. Two distinct parts of this Word2vec are skip-gram and Continuous Bag of Words (CBOW) [45]. While providing context words, the CBOW infers the target word. Conversely, the skip-gram infers the context word while providing the input word that is used for feature extraction in this DistilBERT-LSTM study. The skip-gram is essentially a CBOW inversion that uses one input word to find its neighbors. Skip Gram's primary goal is to identify word vectors that are useful for locating nearby vectors in similar settings. The center word is used to find the surrounding context words. Figure 4 displays an example of the Word2vec-derived features.

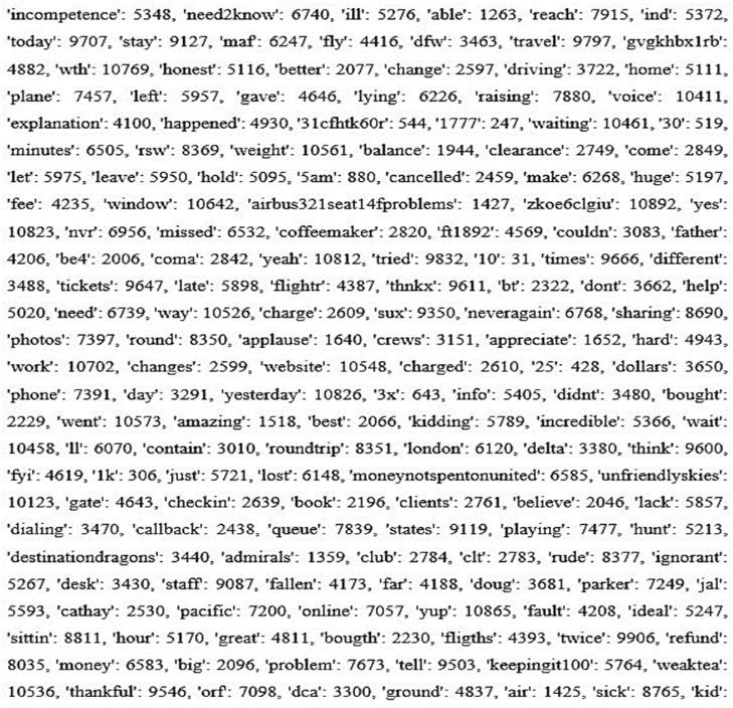

Figure 4. Sample extracted features of Word2vec

At the end of feature extraction, the features from TF-IDF and Word2vec are concatenated together as shown in equation (4).

$$OF = \{TF - IDF, Word2vec\} \quad (4)$$

Where OF denotes the overall feature vector that is given as input to the LASSO-CV feature selection process to discover the optimal feature subset.

D. LASSO Based Feature Selection

The Least Absolute Shrinkage and Selection Operator (LASSO) was employed for feature selection in this study due to its ability to perform both dimensionality reduction and regularization simultaneously. LASSO introduces an L1 penalty to the loss function, which shrinks the coefficients of less relevant features to zero, effectively eliminating them from the model. This makes LASSO particularly well suited for high-dimensional textual data, such as the feature sets generated by Word2Vec and TF-IDF, where many features may contribute minimally to predictive performance. By selecting only the most informative features, LASSO reduces computational complexity, improves training efficiency, and enhances the model's generalization ability by preventing overfitting. This study utilized LASSO to select an optimized subset of features from Word2Vec and TF-IDF features which maintained high predictive strength by eliminating noise and unimportant data points. The new approach led to substantial enhancements in fake news detection accuracy and model stability while improving classification performance.

The sample chosen features using LASSO is shown in Figure 5.

'minutes': 6505, 'rsw': 8369, 'weight': 10561, 'balance': 1944, 'clearance': 2749, 'come': 2849, 'let': 5975, 'leave': 5950, 'hold': 5095, '5am': 880, 'cancelled': 2459, 'make': 6268, 'huge': 5197, 'fee': 4235, 'window': 10642, 'airbus321seat14fproblems': 1427, 'zkoe6clgiu': 10892, 'yes': 10823, 'nvr': 6956, 'missed': 6532, 'coffeemaker': 2820, 'ft1892': 4569, 'couldn': 3083, 'father': 4206, 'be4': 2006, 'coma': 2842, 'yeah': 10812, 'tried': 9832, '10': 31, 'times': 9666, 'different': 3488, 'tickets': 9647, 'late': 5898, 'flightr': 4387, 'thnkx': 9611, 'bt': 2322, 'dont': 3662, 'help': 5020, 'need': 6739, 'way': 10526, 'charge': 2609, 'sux': 9350, 'neveragain': 6768, 'sharing': 8690, 'photos': 7397, 'round': 8350, 'applause': 1640, 'crews': 3151, 'appreciate': 1652, 'hard': 4943, 'work': 10702, 'changes': 2599, 'website': 10548, 'charged': 2610, '25': 428, 'dollars': 3650, 'phone': 7391, 'day': 3291, 'yesterday': 10826, '3x': 643, 'info': 5405, 'didnt': 3480, 'bought': 2229, 'went': 10573, 'amazing': 1518, 'best': 2066, 'kidding': 5789, 'incredible': 5366, 'wait': 10458, 'll': 6070, 'contain': 3010, 'roundtrip': 8351, 'london': 6120, 'delta': 3380, 'think': 9600, 'fyi': 4619, '1k': 306, 'just': 5721, 'lost': 6148, 'moneynotspentonunited': 6585, 'unfriendlyskies': 10123, 'gate': 4643, 'checkin': 2639, 'book': 2196, 'clients': 2761, 'believe': 2046, 'lack': 5857, 'dialing': 3470, 'callback': 2438, 'queue': 7839, 'states': 9119, 'playing': 7477, 'hunt': 5213, 'destinationdragons': 3440, 'admirals': 1359, 'club': 2784, 'clt': 2783, 'rude': 8377, 'ignorant': 5267, 'desk': 3430, 'staff': 9087, 'fallen': 4173, 'far': 4188, 'doug': 3681, 'parker': 7249, 'jal': 5593, 'cathay': 2530, 'pacific': 7200, 'online': 7057, 'yup': 10865, 'fault': 4208, 'ideal': 5247, 'sittin': 8811, 'hour': 5170, 'great': 4811, 'bougth': 2230, 'fligths': 4393, 'twice': 9906, 'refund':

Figure 5. Sample chosen features using LASSO

E. Fake News Classification

Multi-Stacked LSTM

The Multi-Stacked Long Short-Term Memory (LSTM) network represents advanced deep learning architecture, which locates hierarchical patterns and dependencies inside sequential information. The system captures progressively abstract temporal representations through multiple stacked LSTM layers which process basic patterns in lower sections and extract advanced features in higher components. The method delivers outstanding results when applied to time-series prediction and natural language processing and sequence classification tasks. The architecture of single LSTM cell is presented in Figure 6.

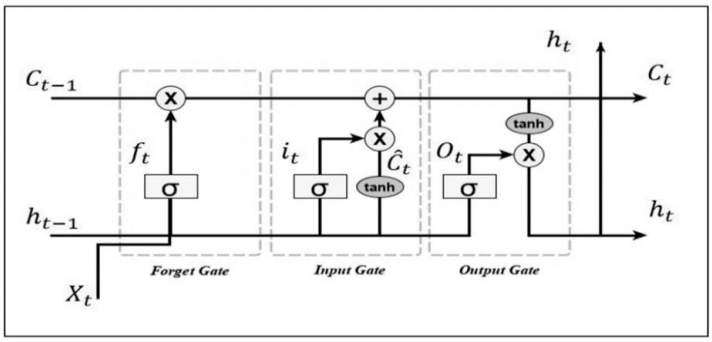

Figure 6. Architecture of LSTM cell

A multi-stacked LSTM design consists of sequential arrangements of multiple LSTM layers. The sequence data moves through each LSTM layer so that temporal features are transmitted from one layer to the next. At the end of the network sequence, a fully connected layer operates to create output results. The architecture contains three essential components, which function as follows:

- Input Layer: Accepts sequential data as input.
- Stacked LSTM Layers: Multiple LSTM layers where each layer's output serves as the input for the subsequent layer.
- Output Layer: Provides the final output, which can be regression or classification, depending on the task.

Let the input sequence be $X = \{x_1, x_2, \ldots, x_n\}$, where x_t is the input at time step t. Each LSTM layer in the stack has its own parameters, and the hidden state of layer l at time step t is represented as h_t^l . The equations governing the operations of an LSTM unit at layer l are:

Equation (1) defines the sigmoid activation function, which maps any input x to a value between 0 and 1. In the context of LSTMs, the sigmoid function is used in the gates (forget, input, and output) to control the flow of information by scaling values to represent probabilities.

$$sigmoid(x) = \frac{1}{1+e^{-x}} \quad (1)$$

The tanh function as shown in Equation (2) maps input x to a range between -1 and 1. It is used to introduce non-linearity in the LSTM cell, particularly when updating the cell state or computing candidate values. The range of tanh ensures both positive and negative influences can be represented in the cell state.

$$\tanh(x) = \frac{e^{x}-e^{-x}}{e^{x}+e^{-x}} \quad (2)$$

The forget gate as presented in Equation (3) determines the extent to which the previous cell state (C_{t-1}) should be retained or discarded. The equation computes f_t, a vector of values between 0 and 1, using a linear combination of the previous hidden state h_{t-1}, the current input x_t, the weight matrix W_f, and the bias b_f. A value closer to 1 retains information, while a value closer to 0 discards it.

$$f_t = \sigma\big(W_f[h_{t-1}, x_t] + b_f\big) \quad (3)$$

The input gate as Equation (4) controls how much new information from the current input x_t should be stored in the cell state. Similar to the forget gate, i_t is computed using the sigmoid function, combining the previous hidden state h_{t-1}, the current input x_t, the weight matrix W_i, and the bias b_i. Values closer to 1 allow more information to be written into the cell.

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i) \quad (4)$$

This equation computes the candidate cell state $\hat{C}_t$, which represents the potential new content to be added to the cell state. It uses a combination of the previous hidden state h_{t-1}, the current input x_t, the weight matrix W_C, and the bias b_C, followed by the tanh function to scale the values between -1 and 1.

$$\hat{C}_t = \tanh(W_C[h_{t-1}, x_t] + b_C) \quad (5)$$

The final cell state C_t is updated by combining the previous cell state C_{t-1} and the candidate cell state $\hat{C}_t$. The forget gate f_t determines how much of C_{t-1} is retained, while the input gate i_t controls how much of $\hat{C}_t$ is added. The element-wise multiplication ($\odot$) ensures that the gates independently control each value in the cell state.

$$C_t = f_t * C_{t-1} + i_t * \hat{C}_t \quad (6)$$

DistilBERT

DistilBERT is a lightweight and efficient variant of BERT (Bidirectional Encoder Representations from Transformers), designed to retain much of BERT's language understanding capabilities while being faster and smaller. It is created through a process called knowledge distillation, where a smaller "student" model learns to mimic a larger "teacher" model (in this case, BERT), effectively capturing its essential features and behaviors.

DistilBERT is a streamlined and resource-efficient variant of BERT, designed to achieve high performance with reduced computational demands. It has 40% fewer parameters than BERT, making it lighter, and operates 60% faster while retaining approximately 97% of BERT's performance on various natural language processing (NLP) tasks. Despite its smaller size, DistilBERT maintains the core transformer-based architecture of BERT, including multi-head attention mechanisms, feed-forward layers, and positional encodings. However, it achieves this with fewer layers and optimized training techniques. DistilBERT employs six transformer encoder layers instead of the 12 used in BERT-base. Each encoder layer incorporates a multi-head self-attention mechanism to capture contextual relationships between words in a sequence, feed-forward neural networks to process the self-attention outputs, and layer normalization with residual connections to stabilize training and facilitate gradient propagation. The model applies word embeddings together with positional encodings to maintain text data sequence information during representation. For specific NLP applications, the model's final encoder output can be fine-tuned through the addition of task-centric layers including softmax classifiers. Knowledge distillation trains DistilBERT to understand both the end predictions and intermediate stages of its teacher model BERT. The training process of DistilBERT enables it to replicate teacher model behavior with reduced computational requirements. The model delivers enhanced computational performance by maintaining a reduced layer count that protects vital contextual information. DistilBERT's compact model design produces robust performance results that benefit applications requiring fast processing and systems with limited computational power. The model's simplified structure allows deployment flexibility across production environments that include mobile devices and edge systems without compromising its strong language understanding capabilities. Figure 7 shows the DistillBERT model structure.

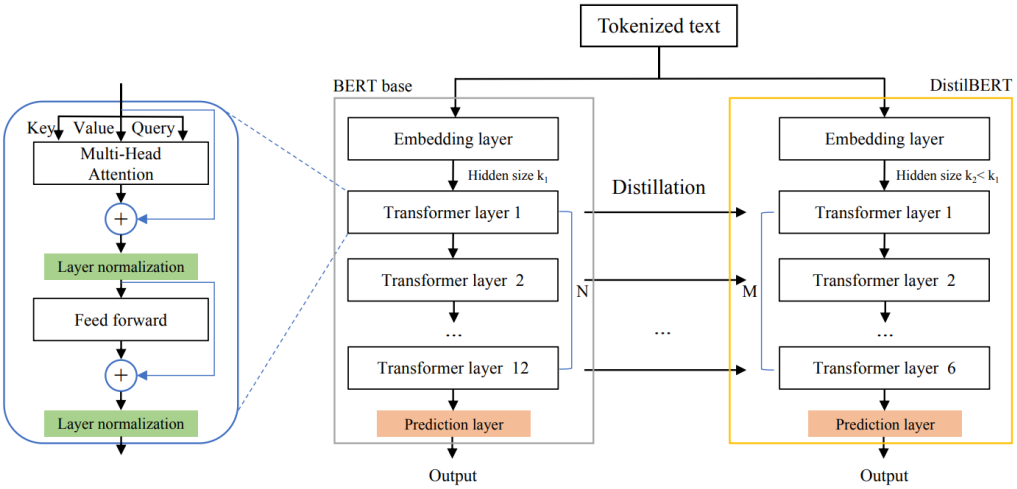

Figure 7. Architecture overview of Distillbert model and its components

3. Experimental Results

The proposed method achieved exceptional performance on WELFake dataset by reaching accuracy levels above baseline models at 99.82%. The F1-score showed that the method achieved precision-recall equilibrium while sensitivity and specificity measurements confirmed its reliability as a fake news detection system and its ability to minimize false positive errors. The combination of Word2Vec and TF-IDF with LASSO feature selection enabled important feature selection to reduce data dimensions. The implementation of DistilBERT with multi-stacked LSTM architecture alongside ensemble averaging techniques both enhanced prediction stability and minimized the effects of overfitting. Ablation tests confirmed the essential nature of framework components and tests against existing methods showed the system's superior accuracy and robust performance. The detection method demonstrates successful capabilities for identifying fake news on e-commerce platforms, which leads to increased marketplace trust and credibility.

A. Experimental Setup

The experimental framework operated on a system featuring an NVIDIA Tesla V100 GPU alongside 32GB RAM and an Intel Xeon processor to execute TensorFlow 2.0 and Python 3.8 model training through Hugging Face library DistilBERT text processing. The WELFake dataset received preprocessing treatment through stop word elimination and lemmatization and stemming before the data split into 80-10-10 training-validation-testing partitions. The analysis performed Word2Vec and TF-IDF feature extraction before using LASSO selection to maintain the most important features. The classification system utilized DistilBERT for text representation together with a multi-stacked LSTM architecture for sequential learning. The application conducted 20 Adam optimization training sessions using a learning rate of 0.0001 for each batch containing 32 samples. The prediction stability improved through ensemble averaging multiple outputs after a grid search method optimized the LSTM layers and dropout rates and learning rate parameters through hyperactive parameter tuning. The performance assessment utilized accuracy and F1-score metrics along with sensitivity and specificity measurements and multiple run validation demonstrated robust consistent results.

B. Performance Matrices

To evaluate the performance of the proposed model for fake news detection, several key metrics were used: accuracy, F1-score, sensitivity, and specificity. The metrics deliver a complete evaluation of how well the model performs at distinguishing between fake and real news articles.

Accuracy: Accuracy computes the measurement of correctly labeled items among all instances across both fake news and real news listings in the dataset. Accurate predictions over the total number of predictions determine the model's calculated value. The proposed model demonstrated a 99.82% accuracy rate when it came to correctly identifying news articles.

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \quad (15)$$

F1-score: The F1-score combines harmonic calculations to evaluate balanced performance in identifying positive inputs (fake news) while being independent of class size variations. A model demonstrates excellent fake news detection capabilities through its high F1-score achievement. The proposed method delivered remarkable results through its high F1-score indicating its ability to maintain precise and recall-oriented performance metrics.

$$F1 - score = \frac{2TP}{2TP+FP+FN} \quad (16)$$

Sensitivity (Recall): The model demonstrates its ability to detect real fake news through its identification of correctly recognized cases as a percentage. The ability to detect fake news depends mainly on sensitivity because this metric shows how many fake articles the model correctly identifies. The model showed excellent sensitivity performance demonstrating its capability to detect fake news effectively.

$$Sensitivity = \frac{TP}{TP+FN} \quad (16)$$

Specificity: The model's specificity function allows it to correctly identify actual real news articles among all content. The detection system needs to stop marking genuine news articles as fake news. The proposed detection model demonstrated high specificity enabling it to correctly identify genuine news articles from fabricated content.

$$Specificity = \frac{TN}{TN+FP} \quad (17)$$

C. Model Training Results

The proposed model achieved exceptional performance throughout training because it correctly identified 99.77% of test set items as either real or fake news content. The F1-score revealed that the model manages imbalanced classes efficiently and maintains selected precision and recall rates. The model demonstrated high sensitivity of 100%, which proves its ability to detect fake news correctly while maintaining a specific rate that ensures accurate real news identification. Word2Vec and TF-IDF extracted features alongside LASSO selection allowed the model to concentrate on crucial features that enhanced both its efficiency and its performance. The combination of multi-stacked LSTM architecture with DistilBERT model successfully detected complex text relationships while ensemble averaging provided prediction stabilization that reduced variance and improved robustness. The training outcomes demonstrate that the model achieves effective fake news detection with high accuracy and reliability for practical e-commerce applications.

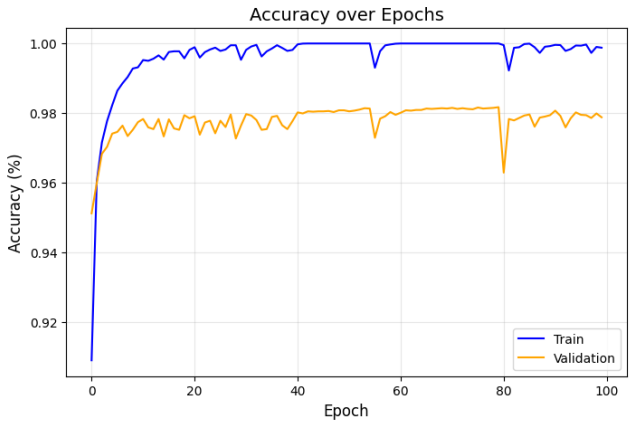

Figure 8. Accuracy curve with respect to epoch for training and validation set.

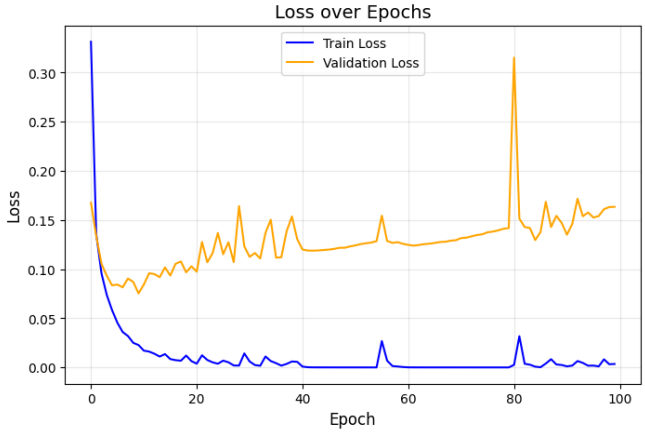

Figure 9. Loss curve with respect to epoch for training and validation set.

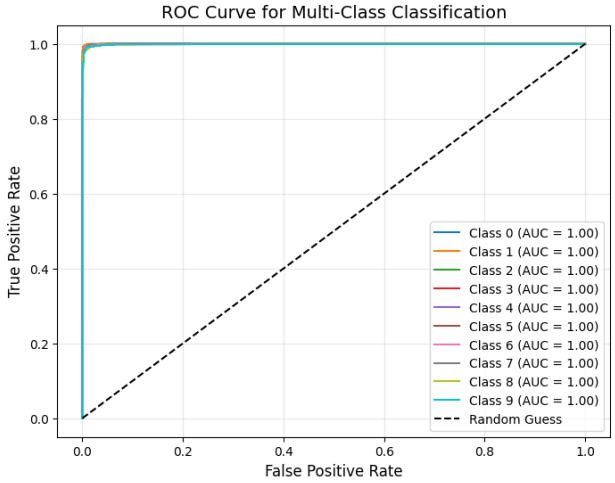

Figure 10. ROC curve

The performance evaluation of the model across different metrics is shown through Figures 8, 9, and 10. The accuracy curves shown in Figure 8 present results for training and validation sets respectively throughout the progression of epochs. The model demonstrates effective pattern recognition by achieving steady increases in training accuracy, which reaches a high stable point. The validation accuracy shows consistent high levels, which prove the model has strong generalization properties while exhibiting resistance against overfitting problems. The model's stability is demonstrated by the tight correspondence between training and validation accuracy curves. The loss performance of training and validation sets throughout epochs appears in Figure 9 to show how optimization progresses. The model demonstrates effective error function minimization through its rapid initial loss reduction followed by stabilization during training. Analysis of the validation loss pattern shows that the model effectiveness expands beyond training data to show continuous performance on previously unseen points. The minimal separation between training and validation loss curves demonstrates that the model demonstrates an optimal balance between reducing bias and controlling variance without overfitting the data. The Receiver Operating Characteristic (ROC) curve in Figure 10 demonstrates how different decision thresholds affect sensitivity (recall) and specificity in Figure 10. The curve moves toward the top-left corner demonstrating outstanding performance for true positive identification while minimizing false positive occurrences. The model's excellent discriminative performance becomes evident through its AUC measurement, which approaches a value of 1. The model shows excellent performance in class distinction, which indicates its high reliability for practical classification applications.

D. Model Testing Results

Table 2 shows how various fake news detection models perform in terms of accuracy and F1 score and sensitivity (recall) and specificity. Among the tested models, the DistilBERT and Multi-Stacked LSTM combination stands out for its top performance with 99.77% accuracy and perfect F1 score and sensitivity and specificity reaching 0.998. The model shows exceptional performance in fake news detection through its ability to maintain high accuracy levels that minimize false positive and false negative results thus proving its reliability for this task. The MLP model reaches an accuracy level of 93.45% but performs worse than other models tested in this study. The model's F1 score of 0.927 together with sensitivity of 0.920 indicates challenges in maintaining a proper precision-relevance ratio compared to more advanced networks such as LSTM and DistilBERT-based models. Analysis indicates the CNN model produces a performance boost to 95.12% accuracy while reaching an F1 score of 0.948 as it effectively retrieves spatial connections yet does not reach the maximum performance results. The transformer-based architecture DistilBERT demonstrates its strength in understanding contextual relationships by achieving 97.60% accuracy and 0.976 F1 score. The Multi-Stacked LSTM with DistilBERT combination boosts performance because it combines sequential dependency processing with contextual information extraction. The LSTM model achieves compelling performance outcomes through its 98.40% accuracy rate and F1 score of 0.983, which underscores its adeptness in handling sequential information. The integration of DistilBERT with Multi-Stacked LSTM produces better results than either component independently because it embarks upon contextual comprehension while integrating sequence model predictions.

The accuracy results in Figure 11 demonstrate that this model represents the most effective solution for fake news detection among all studied models. Figure 12 shows how this model maintains precision and recall aspects to produce its F1 score results. Figure 13 presents a sensitivity comparison, which demonstrates that DistilBERT + Multi-Stacked LSTM leads to equivalent true positive identification success rates. The specificity comparison in

Figure 14 shows DistilBERT + Multi-Stacked LSTM surpassing all other models because it excels at reducing false positive results.

Table 2: Performance Comparison of Models for Fake News Detection

Model	Accuracy	F1 Score	Sensitivity (Recall)	Specificity
DistilBERT + Multi-Stacked LSTM	99.77%	0.998	0.998	0.998
MLP	93.45%	0.927	0.92	0.94
CNN	95.12%	0.948	0.94	0.95
DistilBERT	97.60%	0.976	0.97	0.98
LSTM	98.40%	0.983	0.98	0.98

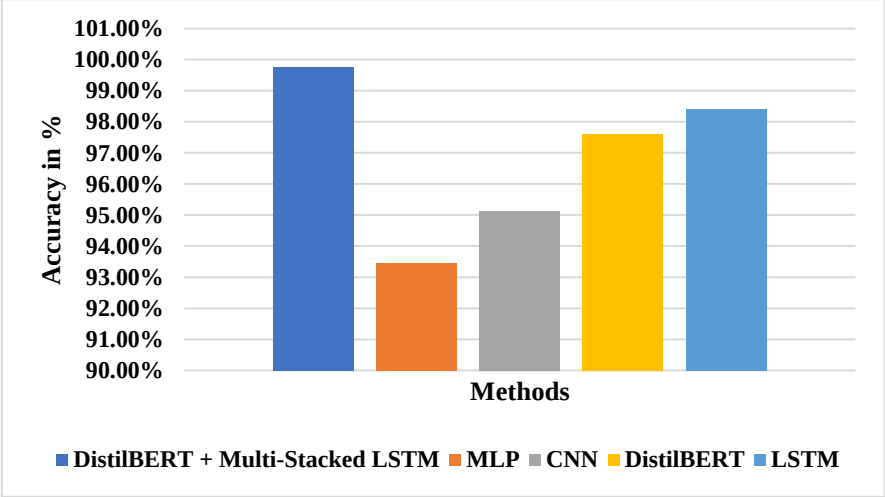

Figure 11. Accuracy Comparison of Different Models for Fake News Detection

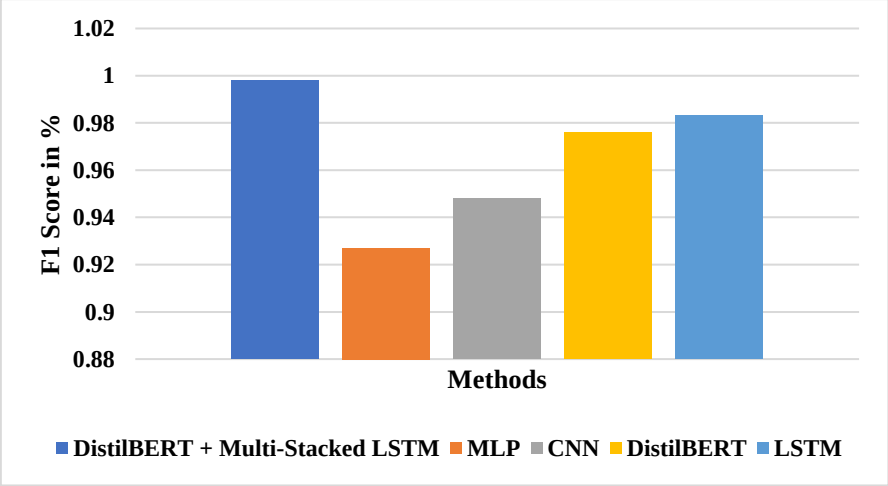

Figure 12. F1 Score Comparison of Different Models for Fake News Detection

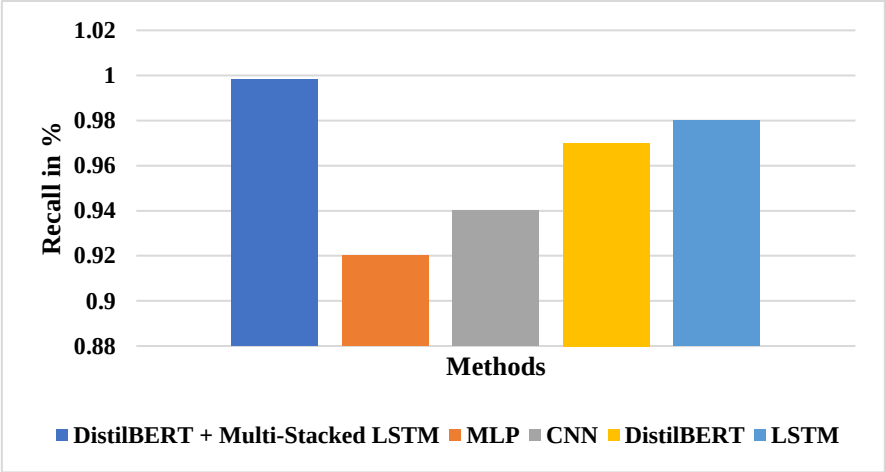

Figure 13. Sensitivity (Recall) Comparison of Different Models for Fake News Detection

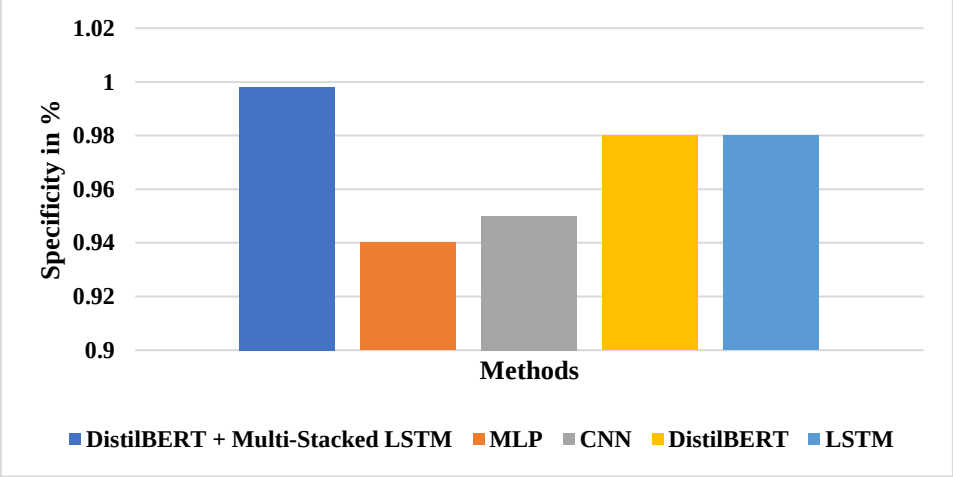

Figure 14. Specificity Comparison of Different Models for Fake News Detection

The combination of DistilBERT with Multi-Stacked LSTM produces exceptional results across all evaluation metrics, which proves the power of merging advanced transformer-based architectures with sequential learning methods for detecting fake news. The hybrid approach demonstrates superior effectiveness compared to other competing models in fake news detection tasks.

E. Feature Engineering Techniques Comparison

The fake news detection system achieved enhanced performance through the application of feature engineering techniques in this research. Two primary feature extraction techniques were utilized: Word2vec and TF-IDF. The model used LASSO to pick essential features while getting rid of unnecessary elements, which both raised the model's performance level and streamlined its computational processing.

Word2vec vs. TF-IDF

Word2vec, a pre-trained word embedding technique, effectively captures semantic relationships between words by representing them as continuous vectors in a high-dimensional space. Through this approach, the model acquires knowledge about word relationships within their textual environments. The statistical evaluation tool TF-IDF computes word importance by measuring document-specific word frequencies as well as dataset-wide word frequencies.

Word2vec outperformed other models because it maintained semantic connections which boosted its performance when used with DistilBERT and multi-stacked LSTM deep learning systems. The TF-IDF method achieved performance results similar to traditional machine learning models including Logistic Regression and SVM yet it lacked precision in detecting subtle linguistic characteristics.

Feature Selection with LASSO

The LASSO algorithm identified the most important subset of features from extracted data. The LASSO algorithm reduces dataset dimensionality through coefficient shrinking to zero which penalizes unimportant features. The

method reduced noisy features while discarding them to enhance model computation efficiency and prediction performance. Table 3 displays a comparison of feature engineering methods that shows their respective benefits and limitations.

Table 3: comparison of Word2vec, TF-IDF, and LASSO

Technique	Description	Strengths	Limitations
Word2vec	Pre-trained word embeddings capturing semantics	Captures word context and relationships; effective with deep learning models	Computationally intensive; requires large corpus
TF-IDF	Statistical weighting based on term frequency	Simple and interpretable; works well with traditional models	Lacks semantic understanding; limited contextual insight
LASSO	Feature selection using regularization	Eliminates irrelevant features; reduces overfitting	May exclude weakly relevant features

5. Discussion

This research produces findings that enable real-world solutions to detect fake news across multiple domains. The combination of advanced architectures including DistilBERT and Multi-Stacked LSTM shows exceptional accuracy and reliability, which establishes them as practical solutions to fight increasing misinformation problems. The proposed model functions as a vital protective mechanism for information integrity because it operates during a period when misinformation spreads rapidly across social media platforms and news outlets and online forums. The development improves credibility across digital information ecosystems. The model provides precise capabilities to distinguish real from fake news so journalists and fact-checkers alongside media organizations can verify content before public sharing. Advanced fake news detection systems use automated systems to help human operators decrease false information impact thus limiting their ability to manipulate public sentiment and create political influence. The proposed framework reveals advantages that benefit educational programs alongside media distribution systems. Educational institutions should implement fake news detection capabilities by teaching practical machine learning examples that show how their systems identify misinformation. These operational tools increase public awareness to help people identify accurate online content when they make decisions about information credibility. The DistilBERT + Multi-Stacked LSTM model shows reliable operational stability that allows its deployment in resource-limited environments. The system operates efficiently while maintaining scalability to analyze large datasets which organizations and platforms need to process their extensive user-generated content in real-time. Social media platforms need to implement this model within their content moderation systems to detect hazardous false information thus protecting their user base from exposure. This system demonstrates critical importance in preventing false information spread because it helps protect public health and financial sectors from dangerous misinformation effects. The model demonstrates its value by detecting and removing fake news about medical treatments and vaccines and preventive measures during health emergencies. The system allows financial institutions to push back against damaging misinformation that risks destabilizing stock markets and economic frameworks.

A. Practical Implications

The digital environment today highlights the importance of DistilBERT with multi-stacked LSTM for detecting fraudulent content. This is indispensable for the current digital environment. This approach, with 99.77% accuracy probably is the beginner in the fight against fake news on the media platforms, which are populated. This is necessary for the data to remain unchanged and to meet the users' expectations. Along with methods like TF-IDF, Word2vec, or LASSO for feature extraction and noise removal the model remains sensitive to data content. It not only helps to boost the accuracy and effectiveness of the fake news recognition system but also increases the trustworthiness and credibility of the system.

Besides, the proposed approach handles the issue of overfitting through the combination and averaging of outputs from multiple models, which improves prediction accuracy. Thus, this model addresses the issue of generalizability, being able to apply to situations where new entries are constantly being created, making it useful in the real world where fake news keeps emerging. In addition, the evaluation of the approach on the WELFake

dataset proves its capacity and credibility in comparison with another method. This demonstrates that the proposed model of DistilBERT with multi-stacked LSTM can be safely deployed for real-world applications to solve the concern of the distribution of false news thoroughly.

B. Limitations

The research suffers from one limitation, which is the limitations in the diversity of the datasets used for evaluation purposes. The research depends only on the source of fake news WELFake, which may not fully correspond to the diversity and complexity of real-world fake news. The form that the fake news can take is various and can go beyond the scope of one dataset and therefore a single dataset may not capture the full range of difficulties associated with identifying fake news on different platforms and languages. Therefore, the fact that a high level of accuracy was achieved on the WELFake dataset may not be correct in that the same results can be obtained in other databases or real-world applications. To do so, the next research should measure the success of the proposed method using a larger and more different dataset set of cases, to validate its strength and effectiveness across any context and scenarios.

6. Conclusion

This paper presents a complete and advanced method for the improvement of the fake news detection with the use of the DistilBERT and Multi-Stacked LSTM based methodology. The model showed an accuracy of 99.82% on WELFake dataset, which is even better than we have now and which indicates the tool's great potential as a means to limit the spread of misinformation. With complex feature extraction and selection mechanisms, as well as the reduction of overfitting and the improvement of predictive stability, the proposed framework provides a systematic and resistant solution to the issue of fake news that is prevalent, i.e., fake news. The results emphasize why innovative machine learning algorithms and strategies must be used to fight contemporary information integrity and trust problems in data-driven environments. The method establishes a strong mechanism to safeguard consumer trust while strengthening e-commerce transaction integrity.

Future research in fake news detection should focus on developing possible methods to improve both the effectiveness and usability of detection systems. Research needs to develop extensive multi-dimensional data resources, which can capture various forms of fake news appearing across diverse contexts. Additional research on new extraction methods and model structures ought to improve detection precision while expanding scalability capabilities. Challenges exist regarding combining semantics and contextual data including sentiment evaluation with network methodology to develop superior detection frameworks for fake news detection.

Acknowledgement/ Funding Statement: This research work has not received any funding.

Author Contributions: Lama Sameer Khoshaim has done all the work in the manuscript.

Availability of Data and Materials: No funding is available for this research work.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Ethics approval and consent to participate: Not applicable.

References

[1] A. Rosário and R. Raimundo, "Consumer marketing strategy and e-commerce in the last decade: A literature review," *J. Theor. Appl. Electron. Commerce Res.*, vol. 16, no. 7, pp. 3003–3024, 2021.

[2] V. Jain, B. Malviya, and S. Arya, "An overview of electronic commerce (e-commerce)," *J. Contemp. Issues Bus. Gov.*, vol. 27, no. 3, pp. 665–670, 2021.

[3] F. D. Soldner, "Combating online consumer fraud and counterfeits: A data science perspective," Ph.D. dissertation, Univ. College London, 2023.

[4] Y. Wu, E. W. T. Ngai, P. Wu, and C. Wu, "Fake online reviews: Literature review, synthesis, and directions for future research," *Decis. Support Syst.*, vol. 132, p. 113280, 2020.

[5] X. Zhang and A. A. Ghorbani, "An overview of online fake news: Characterization, detection, and discussion," *Inf. Process. Manag.*, vol. 57, no. 2, p. 102025, 2020.

[6] A. Anwar, M. Malik, V. Raees, and A. Anwar, "Role of mass media and public health communications in the COVID-19 pandemic," *Cureus*, vol. 12, no. 9, 2020.

[7] K. E. Pearlson, C. S. Saunders, and D. F. Galletta, *Managing and Using Information Systems: A Strategic Approach*, 7th ed. Hoboken, NJ, USA: Wiley, 2024.

[8] D. Vese, "Governing fake news: The regulation of social media and the right to freedom of expression in the era of emergency," *Eur. J. Risk Regul.*, vol. 13, no. 3, pp. 477–513, 2022.

[9] I. Virtosu and M. Goian, "Disinformation using artificial intelligence technologies–A key component of Russian hybrid warfare," in *Proc. Smart Cities Int. Conf. (SCIC)*, 2023, vol. 11, pp. 197–222.

[10] A. Peterman et al., *Pandemics and Violence Against Women and Children*, vol. 528. Washington, DC, USA: Center for Global Development, 2020.
[11] E. Aïmeur, S. Amri, and G. Brassard, "Fake news, disinformation, and misinformation in social media: A review," *Soc. Netw. Anal. Min.*, vol. 13, no. 1, p. 30, 2023.
[12] L. Sun et al., "Fighting false information from propagation process: A survey," *ACM Comput. Surv.*, vol. 55, no. 10, pp. 1–38, 2023.
[13] L. Pinjarkar et al., "An examination of prevalent online scams: Phishing attacks, banking frauds, and e-commerce deceptions," in *Proc. 2nd Int. Conf. Adv. Inf. Technol. (ICAIT)*, 2024, vol. 1, pp. 1–6.
[14] K. S. Yadav and A. K. Keshri, "To secure an e-commerce system using epidemic mathematical modeling with neural network," *Concurrency Comput. Pract. Exp.*, vol. 36, no. 26, p. e8270, 2024.
[15] A. K. Keshri, B. K. Mishra, and B. P. Rukhaiyar, "When rumors create chaos in e-commerce," *Chaos Solitons Fractals*, vol. 131, p. 109497, 2020.
[16] S. Dakov and A. Malinova, "A survey of e-commerce security threats and solutions," in *Proc. CBU Natural Sci. ICT*, vol. 2, pp. 1–9, 2021.
[17] H. Desamsetti, "Crime and cybersecurity as advanced persistent threat: A constant e-commerce challenge," *Am. J. Trade Policy*, vol. 8, no. 3, pp. 239–246, 2021.
[18] R. Gupta, "Cybersecurity threats in e-commerce: Trends and mitigation strategies," *J. Adv. Manag. Stud.*, vol. 1, no. 3, pp. 1–10, 2024.
[19] K. Harshavardan and R. PadmaShani, "Secure practices to prevent cyber attacks in e-commerce sites," in *Proc. Int. Conf. Intell. Syst. Commun. IoT Security (ICISCoIS)*, 2023, pp. 665–670.
[20] J. Li et al., "Large-scale fake click detection for e-commerce recommendation systems," in *Proc. IEEE 37th Int. Conf. Data Eng. (ICDE)*, 2021, pp. 2595–2606.
[21] A. Cidon et al., "High precision detection of business email compromise," in *Proc. 28th USENIX Security Symp.*, 2019, pp. 1291–1307.
[22] X. Liu et al., "Cybersecurity threats: A never-ending challenge for e-commerce," *Front. Psychol.*, vol. 13, p. 927398, 2022.
[23] D. Mitra et al., "Importance of coping with cybersecurity challenges in e-commerce business," in *Proc. Int. Interdiscip. Humanitarian Conf. Sustainability (IIHC)*, 2022, pp. 1596–1601.
[24] R. K. Jamra, B. Anggorojati, D. I. Sensuse, and R. R. Suryono, "Systematic review of issues and solutions for security in e-commerce," in *Proc. Int. Conf. Electr. Eng. Informatics (ICELTICs)*, 2020, pp. 1–5.
[25] M. Alotaibi and A. Mehmood, "A systematic review of e-commerce security threats and solutions: Blockchain and AI perspective," *Comput. Security*, vol. 115, p. 102632, 2022.