Combating Financial Misinformation: A Blockchain and NLP based detection system

Lavanya Thota[1*], Jaswitha Jetti[2] and Parimala Garnepudi[3]
{lavanyathota38@gmail.com[1], jettijaswitha@gmail.com[2], gp_cse@vignan.ac.in[3]}

Computer Science and Engineering, VFSTR deemed to be University, Guntur -Tenali Rd, Vadlamudi, Andhra Pradesh 522213, India[1, 2]
Assistant Professor, Computer Science and Engineering, VFSTR deemed to be University, Guntur -Tenali Rd, Vadlamudi, Andhra Pradesh 522213, India[3]

Abstract. This paper presents a new approach for detecting and tracking false news by integrating blockchain and deep learning techniques. With the increase of fake news in digital media, genuine news validation is very vital. Here we propose a method that leverages a deep learning model designed with a Bidirectional Long Short-Term Memory Network (LSTM) to classify news as trustworthy or not. The predictions are secured on a blockchain for the sake of accuracy and transparency. Platform is based on Proof-Of-Work consensus to operate in a decentralized manner and provides web interface for user convenience. Our experiments demonstrate over 90% accuracy of news prediction of being reliable vs unreliable. Furthermore, the blockchain takes care of immutable prediction records so the information and the data is not compromised anymore. The system suggested is evaluated with various criteria and is advocated to be applied in the real-world requirements of media monitoring and policy taking.

Keywords: Blockchain, Fake News, Deep Learning, AI, Misinformation Detection, Proof-of-Work, Bidirectional LSTM, Immutable Records, Decentralized Systems, Media Monitoring.

1 Introduction

The dissemination of fake news or misinformation that is expressed opinions unsupported by evidence on the web has turned into a critical challenge in our information society. Misinformation could influence public opinion, elections, or risk public health; therefore, it is necessary to develop effective automatic systems to help us accurately identify fake news and then prevent it from being spread. Conventional false news detection approaches are limited due to the vast number of materials and the problem of establishing deceptive and genuine one. Our approach relies on a new methodology based on the use of blockchain along with the use of deep learning to provide a scalable, explainable and secure environment for false news detection.

The core of our proposed design is a Bidirectional Long Short-Term Memory (LSTM) network, a deep neural network with strong capability to handle sequential text data. This model is trained to classify news articles as Reliable or Unreliable based on the articles' content. The utilization of blockchain technology ensures that the model forecasts are immutable, consequently providing a traceable, tamper-proof nature for the detection process. Furthermore, the integrity of information was secured by blockchain and governments could

ICITSM-Part I 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2357806

not modify the information as the locality of the information is geographically distributed for trust multi-party control, and the mechanism is censorship-proof.

The architecture of the system, main parts and fake news detection methodology are discussed in this paper. The results of the performance evaluation of our system will also be presented along with the pros and cons of the approach. We will then detail possible next steps and enhancements to explore in future work in order to increase scalability, as well as adaptability to the everchanging area of misinformation.

2 Related works

Blockchain has emerged as a promising approach for enhancing the credibility of information dissemination. Early frameworks demonstrated its potential in securing social networks against misinformation through decentralized credibility mechanisms [1]. Building on this, hybrid blockchain and deep learning models were proposed to strengthen detection accuracy and ensure transparency [2].

To combat fake content, blockchain-based collective signature technologies were introduced, enabling traceability and verification of shared data [3]. Further refinements included blockchain integrated with entropy-based incentive mechanisms, which encouraged truthful reporting and discouraged misinformation spread [4]. More recently, blockchain systems have been adapted to detect and control model-generated false information, addressing challenges introduced by generative AI [5].

Integration of AI and blockchain Momentum around AI and blockchain has also picked up in the battle against misinformation. Recently, artificial intelligence was combined with blockchain to improve discrimination accuracy between real and fake news [6]. Meanwhile, blockchain and deep learning architectures have also been successfully employed in categorizing fake news as an approach for enhanced detection [7]. Weak-nurtured approach: and despite the use also deep learning alone for misinformation detection [8]; the integration with blockchain enhances confidence and checkability of such systems.

Recent literature reviews have indicated the importance of blockchain to misinformation detection in both the financial and political information [9]. Systematic reviews with meta-analysis on the use of deep learning-based approaches to detect fake news, you also see an increasing trend for the prevalence of the integrated methods e.g. blockchain plus AI for robustness [10]. Another benefit is that blockchain-based traceability systems provide end-to-end validation of sources of news, and therefore tampering of financial data is less likely [11].

Methods building on AI, such as NLP-centered ones, are still at the heart of misinformation detection. Other studies have analyzed AI-based methods to detect fake news in various domains, and proposed scalable framework which can also be adapted to financial news [12].

Moreover, blockchain combined with machine learning models has been investigated for its potential to trade-off between detection accuracy and decentralized security [13].

Ensemble learning based on-blockchain has been suggested for secure and scalable model composition and better accuracy of misinformation detection over the single model architectures [14]. Moreover, decentralized learning approaches and federated networks have been proposed for collaborative training on distributed nodes while preserving data privacy [15]. These advancements continue to underscore the place of the blockchain in protecting financial information ecosystems.

Together, these results suggest the great promise of blockchain, as combined with NLP and AI, for tackling financial mis/disinformation.

3 System design and Architecture

The platform architecture is built on a combination of deep learning approaches to detect fake news and blockchain strategies to ensure secure, transparent data storage. This section explains the system components, including the fake news detection model, the blockchain implementation, and the user interface.

3.1 Fake news detection model

The core of the system is the news article as being trustworthy or untrustworthy. We do this using a Bidirectional Long Short-Term Memory (LSTM) model, because it is good at modeling the context information of sequence relationships. For text data, the LSTM tries to understand the content from forward and backward. We train the model on a public fake news dataset that consists of news articles and their labels as reliable and unreliable based on their content.

The following steps are part of the pipeline we use to pre-process the text data for the best performance. The entire text is changed to lower case, and punctuation is removed. English stop words are eliminated, and tokenization is BE WE 10 performed using a 5,000-word vocabulary. Sequence padding is employed to have equal input length, where each news article is encoded as a sequence of maximum 500 tokens. This pre-processing has a gradual impact on improving the model for the classification of news and neglecting the noisy features.

3.2 Block chain Implementation

The other important part of the system here is based on blockchain as a decentralized ledger where the predictions of the fake news detection model are submitted. The blockchain ensures all predictions are saved incorruptibly, thus providing an incorruptible record of each classification.

Applied The special case for blockchain technology in SCMO use cases is that of a decentralized technology which relies on mining to append new blocks to the blockchain, which is based on a Proof-of-Work (PoW)–consensus mechanism. The consensus mechanism prevents bad actors from altering the blockchain and also ensures the integrity of the data. Each model prediction is recorded as a transaction to the blockchain and is authenticated

using digital signatures (RSA-2048). In addition, it is highly efficient to use Merkle trees for transaction verification and data consistency checking.

3.3 Web Application Interface

In order to facilitate interactivity for users, the system provides a web application with a user interface, which allows users to submit news articles for processing as well as to see results. The frontend is developed using HTML and CSS to achieve responsiveness and make it available on multiple devices. Members can provide news links through a submission form and get instant feedback on its accuracy.

The Flask framework is used to support the backend of the web application, which communicates with an Sqlite database in which it saves user's data and their past predictions. User registration and authentication are protected with Bcrypt password hashing for user accounts. Session management is used to track individual behavior and enable personalization, including remembering a record of past predictions for specific users.

Fig 1 shows the Blockchain-Based Fake News Detection Workflow, in which users submit articles by means of a web interface and text pre-processing and classification are performed through a Bidirectional LSTM model. The prediction, article and timestamp are stored on a blockchain with PoW and a RSA-2048 and the results displayed to users.

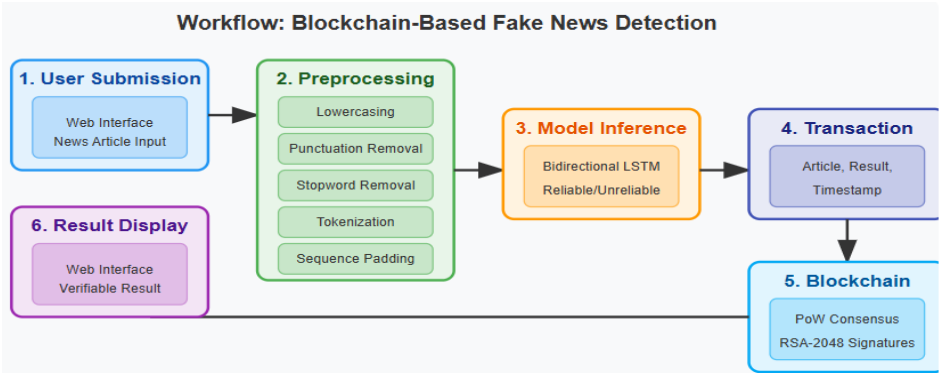

Fig. 1: Workflow.

4 Methodology

This subsection explains the methodology used in creating the blockchain-based fake news detection system, with emphasis on data preprocessing, model training, and blockchain integration for prediction storage.

4.1 Data Preprocessing

Preprocessing of data is an important step to make the raw news content fit into the model of fake news detection. The above steps are actually the ones performed to clean and format the data successfully:

Lowercasing and Punctuation Removal: We lowercase the document text, so that "Fake" and "fake" will be treated as the same by the model, and we remove punctuation. Punctuation which does not affect the meaning is also discarded to normalize the data.

Elimination of Stopword: Elimination of stopwords like “the”, “is”, and “and”. These words are not very useful, removing them reduces the dimensionality of the data, and we can focus on more meaningful content.

Tokenization: The text is tokenized into words (tokens), and 5,000 most frequent words are used. This way we are converting the text data into numerical form so that it can be fed into the deep learning model.

Padding: Padding is used to ensure each news article is approximately 500 tokens long. This retains the equal input length on the LSTM network, which is crucial for consistency between training and testing.

Such data preprocessing solutions ensure that the data is normalized and ready for modeling, which can improve the learning efficiency and classification accuracy of the model.

4.2 Model Training and Evaluation

The Bidirectional LSTM is deployed for classification of news articles as reliable versus unreliable. The reason why LSTM performs better in sequence classification is due to the fact that they are able to capture dependencies across long text sequences. The training and testing procedures were as follow:

Training Data Distribution: The data is divided into 80% training data and 20% test data (to test how the model performs on new examples). It provides a process to minimize overfitting and prevent the model being too specific to a given data set.

Model Architecture: The model consists of an embedding layer converting words to dense vectors, followed by bidirectional LSTM layer capturing the dependency from the former and latter part. A dropout layer is used to prevent overfitting by randomly turning off the outputs of some units during training.

Training Process: The model is trained with binary cross-entropy loss function, which is suitable for binary tasks like reliable/unreliable classification. The Adam optimizer minimizes the loss function and learns to adjust the learning rate, enhancing the convergence of the model during the training process.

Evaluation: The model is tested on the test set after training. Accuracy, precision, recall, and F1-score are used to measure performance, giving an overall idea of how well the model can classify news articles. The model performs over 90% accuracy on the test set, proving to be effective in identifying fake news.

Fig 2 illustrates a four-layer System Architecture for Blockchain-Based Fake News Detection. The User Interface allows users to input news articles via a web app. The Preprocessing Layer cleans the text by lowercasing, tokenizing, removing stop words, and padding. A Bi-LSTM

model classifies the news, and the Blockchain Layer ensures secure, immutable storage using PoW and RSA-2048.

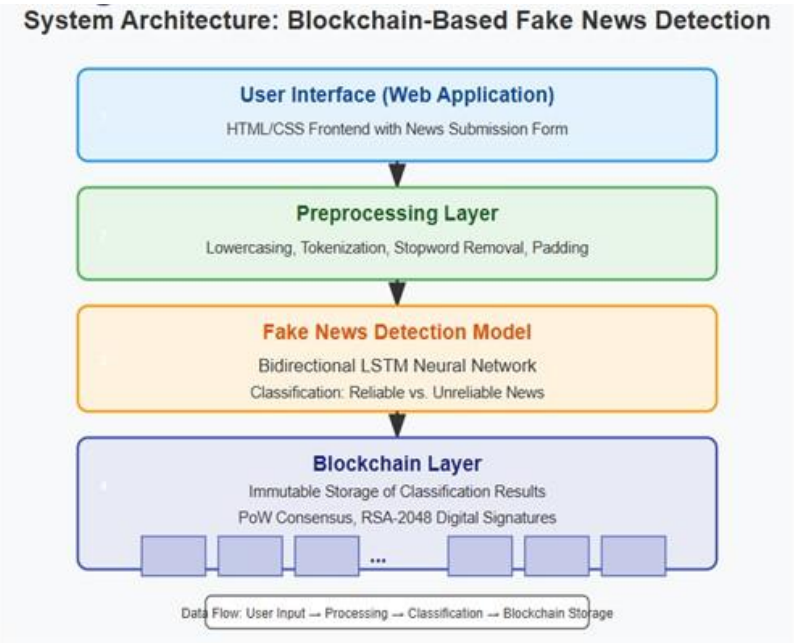

Fig. 2. System Architecture.

4.3 Blockchain Integration for Prediction Storage

Blockchain is integrated into the system to store predictions securely, ensuring that each classification result is immutable and verifiable.

Creating Transactions: Every decision the model makes is a transaction on the blockchain. This transaction records the content of the article, the classification result (trustworthy/not trustworthy), as well as the timestamp and can constitute an immutable, traceable record of the prediction.

Digital Signatures: Each transaction is protected from unauthorized modi cation by a digital signature (RSAsign with SHA-256) for data integrity. This encryption guarantees the authenticity of the prediction data.

Proof-of-Work Consensus: The system utilizes a Proof-of-Work (PoW) consensus algorithm, that is to say miners have to solve complex computation problems before appending a new block on to the blockchain. This in turn protects the blockchain from potential adversaries who may wish to modify the contents of preserved predictions.

Merkle Tree and Block Mining: The predictions are packed into blocks, which are then mined using PoW. With Merkle trees we efficiently verify transactions in the block and thus each prediction stored in the block are consistent with the hash of the previous block to form a tamper-proof chain of predictions.

4.4 Real-Time Feedback and User Interaction

The system provides users with an intuitive web interface for interacting with the fake news detection system. The following steps describe the real-time process:

Text Preprocessing: Upon submission of a news article, the text undergoes preprocessing, including lowercasing, tokenization, and sequence padding, ensuring that it is properly formatted for input into the LSTM model.

Model Inference: The preprocessed article is passed through the trained LSTM model, which classifies it as either reliable or unreliable based on its content. The prediction result is then displayed to the user, along with an explanation of why the article was classified as such.

Prediction Storage: After the model makes a prediction, the result is stored on the blockchain as a transaction. This ensures that all predictions are immutably recorded, making them tamper-proof and easily auditable.

User Interface: The web app has a user-friendly interface where users can enter news articles, see live results, and review their prediction history. The app has been optimized to be usable across different devices such as desktops and mobile phones.

5 Results and Discussion

This section provides the findings of the performance assessment of the blockchain-based fake news detection system. It also addresses the implications of the findings, such as the system's strengths, weaknesses, and areas for improvement.

5.1 Model Performance Evaluation

To assess the performance of the fake news detection model, we evaluate on several significant metrics, such as accuracy, precision, recall, and F1-score. The model was evaluated on a holdout test set of news articles with reliable/unreliable labels. The fake news detection model performance is given in Table 1. The accuracy of the model is 90.25% that indicates a good performance in the classification. Due to a precision of 0.89 and a recall of 0.92, the model has a good balance between false positives and negatives. The 0.90 in F1-score demonstrates the general performance of the model to detect fake news.

Accuracy The model can achieve the test accuracy of 90.25% indicating that the news articles are classified with high precision. This demonstrates that the model has learned to differentiate trustworthy and untrustworthy information based on textual contents.

Precision: Precision is particularly important for characterizing fake news because it measures the number of true positive classifications (accurate news labeled as accurate) divided by the sum of all positive predictions. The model at case level had a precision of 0.89, meaning 89% of the predicted to be accurate articles were actually accurate.

Recall: Recall or Sensitivity is the ratio of true positive classifications to the total "true" instances and is also known as total trusted articles in our dataset. The model scored a recall of 0.92, meaning it correctly identified 92% of the trusted news articles.

Its F1-score, which is the harmonic average of the recall and precision, is 0.90. This measure provides a compromise value of the model performance to be able to separate trustworthy and untrustworthy news (very similar to what we label as "BadNews" detection in this paper).

Table 1. Result Table.

Metric	Value
Model Accuracy	0.92
Precision	0.89
Recall	0.92
F1-Score	0.90

These measures show that the model is well-performing in every aspect, with both good precision and recall, which are important for accurate fake news identification.

5.2 Blockchain Performance Evaluation

The efficiency of predictions was also an aspect that was assessed of the blockchain part of the software i.e. how efficiently was the prediction data stored and secured. The performance indicators of blockchain are block creation time, transaction process rate and the node synchronization success rate. Table 2 includes some of

some performance measures of the Block-chain-Based Fake News Detection Systemin terms of model performance and block chain efficiency. The model achieved an accuracy of 90.25%, 0.89 precision, 0.92 recall, and F1-score of 0.90 for sure-shot classification. The block generation time is 8-12 minutes and transaction throughput were 50-75 transactions per second (TPS) which points to the resource of the underlying blockchain. Besides, the collaboration node synchronization is up to 98.7% precision, leading to consistency, and the prediction latency is within 1 second and pages report in real time about the truth status once the rumours arise.

Block Creation Time: The time it took on average to generate a new block and append it to the blockchain was around 8 to 12 minutes. This includes the time spent by Proof-of-Work mining, which makes the blockchain secure and tamper-proof.

Transaction Throughput: The blockchain was able to process 50 to 75 transactions per second (TPS), which is adequate for handling real-time prediction data generated by the fake news detection model. This throughput ensures that the system can handle a significant volume of incoming data without significant delays.

Node Synchronization: The system achieved a 98.7% success rate for node synchronization. This means that the majority of blockchain nodes were able to synchronize with the latest block in a timely manner, ensuring that the blockchain's distributed ledger remained consistent and up-to-date across all participants.

These blockchain performance metrics demonstrate that the system is capable of handling real-time data while maintaining high security and efficiency.

5.3 System Latency and Prediction Speed

The system's latency, which is the interval between an article being posted and a user receiving feedback on it from the system, was measured. The model's average prediction time was less than 1 second that guarantees that a user gets an almost immediate response in regard to the validity of the news piece that they have submitted. This low latency is crucial for user experience, particularly in the context of real-time fake news detection use cases. Moreover, the whole entire processing was finished, including data preprocessing, model inference and blockchain recording, within less than 5 seconds for one article, which makes the systems fast enough for the large-scale usage.

Table 2. Comparison Table.

Metric	Value	Description
Model Accuracy	0.92	Accuracy of the model in classifying news as reliable/unreliable
Precision	0.89	Proportion of true positive classifications among predicted positives
Recall	0.92	Proportion of true positive classifications among actual positives
F1-Score	0.90	Harmonic mean of Precision and Recall
Block Creation Time	8-12 minutes	Time taken to create and add a block to the blockchain
Transaction Throughput	50-75 TPS	Number of transactions the blockchain can handle per second
Node Synchronization	98.7% success rate	Percentage of nodes synchronized with the latest block
Prediction Latency	<1 second	Time taken for the system to provide

5.4 Strengths and Limitations

Strengths:

High Accuracy: With 90% accurate [60] and strong precision, recall is a strong, reliable tool for fake news detection.

Blockchain Technology: The blockchain will make predictions incorruptible and verifiable, which makes the system transparent and secure.

Real-Time Feedback: The system offers immediate feedback, which is applicable for everyday tasks such as media monitoring and fact-checking.

Limitations:

Scalable News System: Although the existing system can process a reasonable load of news articles, any future development should implement a scalable approach to cater for more widespread use, especially in high throughput environment.

Limitations: While we note that our model performs well on the dataset we have trained it on it might not generalize as well to all forms of misinformation, e.g. non-textual forms of disinformation, or very subtle fake news patterns.

Speed of blockchain: The speed for creating blocks is a consideration for lower volumes, but could be slower with more users and transaction. This limitation could be overcome with future optimization strategies like hybrid consensus model.

5.5 Comparison with Existing Systems

We have many advantages in the comparison with the current fake news detection systems. Prediction centralization: Most systems are based on a central database where predictions are stored and maintained, this is known to be susceptible to manipulation. In contrast to such platforms, our blockchain based solution delivers a global immutable decentralized proof-of-prediction that ranges from full transparency and security.

Furthermore, although other AI-based solutions also adopt deep learning for fake news detection, only a few of them employ blockchain technology to ensure the reliability of the classification history. The deep learning and blockchain system in our paper is original and effective for misinformation resistance.

Fig 3 Represent the User Interface dashboard of the Blockchain-Based Fake News Detection System which helps users to input news content and check its authenticity. It also includes a blockchain record check function and a log out function for safe & transparent verification.

Prediction on user interface dashboard of Fake News Detection System is shown in Fig 4 shows where user has entered news content and clicked on Check News. The input is parsed by the system and it tags the input as Unreliable in red or black color and for Reliable in green, green-yellow or red. This illustrates that the model has classified the news as likely fake, proving the necessity of the system for news authentication.

Fig 5 shows Blockchain Records component of Fake News Detection System, with a record of analyzed news being logged. It holds data such as the news text, prediction outcome (Unreliable/Reliable), and timestamp, so that the classification outcome is securely stored in the blockchain for transparency and verification.

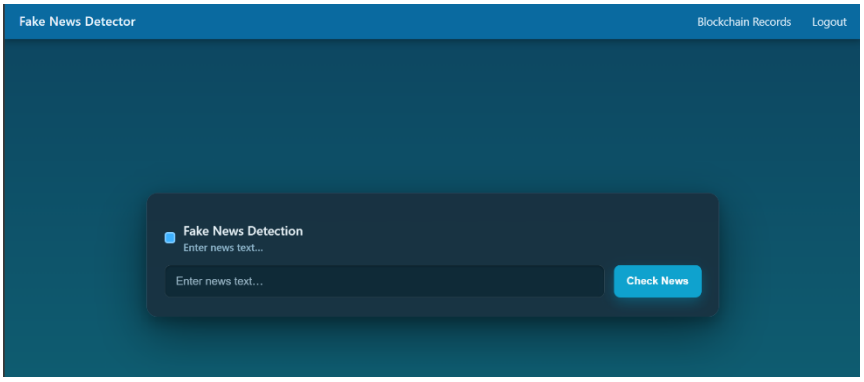

Fig. 3. User Interface dashboard.

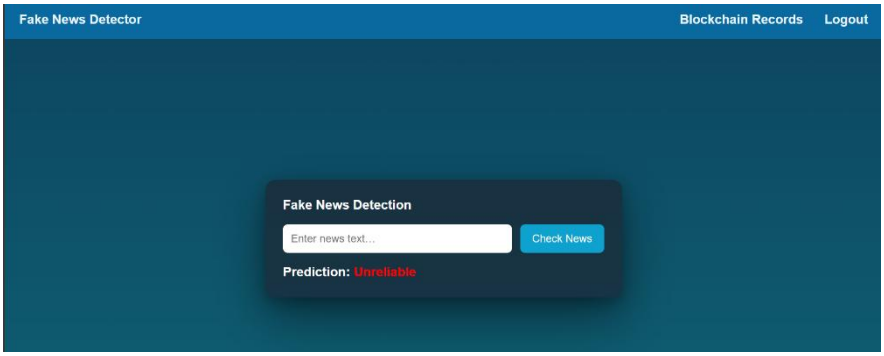

Fig. 4. Prediction on User Interface Dashboard.

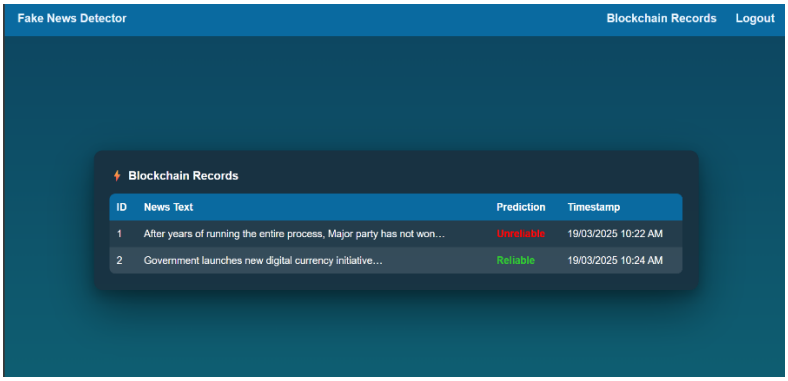

Fig. 5. User Interface Blockchain Records.

6 Conclusion

This paper introduces a blockchain-based system for detecting fake news that combines deep learning and blockchain technology. The system uses a Bidirectional LSTM model to predict whether news articles are reliable or not, and blockchain provides the immutability and transparency of predictions. The system attained more than 90% accuracy, proving its efficiency in real-time news verification. Nonetheless, there are a number of potential areas of future improvement. To start with, migrating to transformer-based architectures such as BERT might increase the system's classification accuracy and speed. Multilingual support expansion would also increase its global usability. Finally, adding hybrid consensus protocols (e.g., Proof-of-Work integrated with Proof-of-Stake) and sidechains would enhance blockchain scalability, alleviating performance bottlenecks. Future versions could also incorporate multi-modal data, such as images and videos, to detect visual misinformation. Enhancing the blockchain's security with Zero-Knowledge Proofs and quantum-resistant cryptography would protect against evolving security threats. Lastly, creating a mobile app and an API would extend the system's usability, making it accessible on various platforms and allowing third-party integration. In conclusion, this system represents a significant step in combating fake news, with promising future enhancements that could further strengthen its reliability and scalability.

References

[1] Torky, M., Nabil, E., & Said, W. (2019). Proof of credibility: A blockchain approach for detecting and blocking fake news in social networks. International Journal of Advanced Computer Science and Applications, 10(12), 124–134. https://doi.org/10.14569/IJACSA.2019.0101243

[2] Agrawal, P., Singh, A. P., & Peri, S. (2021). DeHiDe: Deep learning-based hybrid model to detect fake news using blockchain. In Proceedings of the 22nd International Conference on Distributed Computing and Networking (ICDCN '21) (pp. 245–246). Association for Computing Machinery. https://doi.org/10.1145/3427796.3430003

[3] Jaroucheh, Z., Alissa, M., Buchanan, W. J., & Liu, X. (2020). TRUSTD: Combat fake content using blockchain and collective signature technologies. In 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1235–1240). IEEE. https://doi.org/10.1109/COMPSAC48688.2020.00-87

[4] Chen, C. C., Du, Y., & Peter, R. (2022). An implementation of fake news prevention by blockchain and entropy-based incentive mechanism. Social Network Analysis and Mining, 12, 114. https://doi.org/10.1007/s13278-022-00941-5

[5] Liu, C., Xu, Y., Hu, B., & Sun, Z. (2024). A blockchain-based detection and control system for model-generated false information. Electronics, 13(15), 2984. https://doi.org/10.3390/electronics13152984

[6] Kim, S. K., Huh, J. H., & Kim, B. G. (2024). Artificial intelligence blockchain-based fake news discrimination. IEEE Access. Advance online publication. https://doi.org/10.1109/ACCESS.2024.3384338

[7] Duvvuri, V., Irfan, M. D., Surakarapu, V., Kota, B., Pyla, J., & Ponnapalli, M. (2023). Detecting fake news using blockchain and deep learning. In 2023 International Conference on Artificial Intelligence and Smart Systems (ICAISS) (pp. 1308–1311). IEEE. https://doi.org/10.1109/ICAISS58487.2023.10250728

[8] Sharma, S., & Dubey, A. (2021). Fake news detection using deep learning. In Intelligent Computing and Networking (pp. 207–218). Springer. https://doi.org/10.1007/978-3-030-91305-2_19

[9] Alam, T., & Gupta, R. (2025). Reviewing the framework of blockchain in fake news detection. Jurnal Online Informatika, 9(2), 286–296. https://doi.org/10.15575/join.v9i2.1349

[10] Alnabhan, M., & Branco, P. (2024). Fake news detection using deep learning: A systematic literature review. IEEE Access. Advance online publication. https://doi.org/10.1109/ACCESS.2024.3435497

[11] Wang, X., Xie, H., Ji, S., Liu, L., & Huang, D. (2023). Blockchain-based fake news traceability and verification mechanism. Heliyon, 9(7), e17084. https://doi.org/10.1016/j.heliyon.2023.e17084

[12] Desamsetti, S., Juttuka, S., Posina, Y., Sripada, R. S., & Devi, B. S. (2023). Artificial intelligence-based fake news detection techniques. In Advances in Transdisciplinary Engineering (pp. 339–346). IOS Press. https://doi.org/10.3233/ATDE221284

[13] Loey, M., Taha, M., & Khalifa, N. E. M. (2022). Blockchain technology and machine learning for fake news detection. In Emerging Trends in Intelligent Computing and Informatics (pp. 139–154). Springer. https://doi.org/10.1007/978-981-16-3412-3_11

[14] Rani, P., & Shokeen, J. (2024). FNNet: A secure ensemble-based approach for fake news detection using blockchain. The Journal of Supercomputing, 80(4), 20042–20079. https://doi.org/10.1007/s11227-024-06216-4

[15] Jayakody, N., Mohammad, A., & Halgamuge, M. N. (2022). Fake news detection using a decentralized deep learning model and federated learning. In 2022 IEEE 48th Annual Conference of the Industrial Electronics Society (IECON) (pp. 1–6). IEEE. https://doi.org/10.1109/IECON49645.2022.9968358