

Adversarial-resilient iot-enabled financial intelligence system using explainable deep learning for sentiment-driven stock trading decisions

Suresh Talamala¹, Sukhada Aloni², J. Vijayalakshmi³, Subham Pankaj Samantaray⁴,
K. Swanthana⁵, Nisarg Gandhewar⁶

¹School of Business, Aditya University, Kakinada, India

²Department of Computer Engineering, A. P. Shah Institute of Technology, Thane (West), Maharashtra, India

³Department of Artificial Intelligence and Data Science, St Joseph's College of Engineering, OMR, Chennai, India

⁴Department of CSE, Nigam Institute of Engineering and Technology, NIET, UG PG Diploma Engineering, Odisha, India

⁵Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, India

⁶Department of AIML, Ramdeobaba University, Nagpur, India

Article Info

Article history:

Received Jan 8, 2026

Revised Aug 27, 2026

Accepted Sep 3, 2026

Keywords:

Adversarial attacks

Deep learning

Feature selection

Financial industry

Hyperparameter tuning

IoTs

Sentiment analysis

SHapley additive explanations

Stock market

ABSTRACT

Financial stock market trend decision systems support the investment decisions by predicting future price movements and analyzing large-scale market data. Despite, IoT enabled trading systems continuously collects and exchange sentiment and market information are exposed to adversarial attacks, which misleads automated trading algorithms and results in inaccurate investment decision systems. To face this challenge, this study proposes an adversarial-resilient explainable artificial intelligence for sentiment-driven stock trading (ARXAI-SST) architecture. The proposed framework combines graph neural networks (GNN) for adversarial attack detection, FinBERT based sentiment representation, BiLSTM with attention (BiLSTM-Att) for the sentiment analysis, and SHAP-based explainable artificial intelligence for enhancing model interpretability. The experimentation outcomes show that the proposed framework accomplishes higher accuracy and robustness compared with the existing approaches while providing transparent insights into the trading decisions. The proposed model offers an efficient and reliable solution for secure sentiment driven stock trading in IoT enabled financial environments.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Suresh Talamala

School of Business, Aditya University

Surampalem, Kakinada, Andhra Pradesh - 533437, India

Email: dr.sureshsony@gmail.com

1. INTRODUCTION

With the fast expansion of the IoT, many devices are connected to the IoT [1]. These IoT devices will produce a massive quantity of data that can consume a high amount of computing and storage resources of an IoT. Therefore, the purpose is to require lower delay, wider connection, and better control of cloud computing in IoTs, which is evolving into a worldwide distributed network [2]. Due to the difficulties of existing network security in IoTs, the classical security technology is ineffective. Also, the eruption of increasing network data raises new needs for the study of network security. Malicious attacks on language systems have developed a significant study focus in natural language processing (NLP), particularly concerning large language models (LLMs) [3]. These attacks exploit weaknesses in methods to deceive predictions, with possibly severe consequences in perceptive fields like finance, where attacks can lead to

disrupting business processes, breaking data privacy, spreading misinformation, and financial losses [4]. Consequently, one needs to understand the flaws of these methods to recognise and moderate their vulnerabilities. Financial sentiment analysis techniques that can extract importance from vast quantities of raw data act as a vital part in sentiment-based financial decisions [5]. Stock prediction has a high significance in the financial domain. During the stock fluctuation, which is very impulsive, research workers have made every effort to imitate the stock difference since a comparatively sensible prediction can make huge profits and help decrease risks [6]. Economic conditions, Investors' sentiments, and public sentiments are all essential variables that must be supplemented into a stock prediction model [7]. Especially, sentiment analysis (SA) was recognised as an effective tool in the last few years. Not just price and price-related values, research workers have paid more consideration to the extraction of sentiment data from journals, newspapers, and also social media [8]. Adversarial attacks in machine learning (ML) methods are a primary concern, as these attacks may seriously affect the performance of even the most developed systems [9]. These attacks have several methods and types, such as evasion attacks, where an attacker deploys the input data to poison attacks or avoid detection [10].

Kim *et al.* [11] presented a stock trading suggestion method, which combines relative strength index (RSI) with the news SA for providing knowledgeable buy–sell decisions. This method employed a rule-driven NLP technique to analyse the current newspaper reports and integrates the consequent sentiment scores among the RSI that can follow the stock level. The above-mentioned method allocates a sentiment score that replicates market sentiment, while the RSI detects oversold or overbought states. This integrated method enables traders to create data-based sell, buy, or hold decisions in real life. Narayana *et al.* [12] produced a hybrid composite method, which integrates traditional stock market estimation systems through SA of news articles to escalate the prediction accuracy. Through the benefits of a collaborative architecture, the method's capability to suit the varying requirements of investors provides the best results it has attained over risk profiles. Pandiri *et al.* [13] developed a method for analysing the perspective of recurrent neural networks (RNNs) in performing SA of financial information for improving the market prediction and improving investment methods. Therefore, using these advanced NLP techniques and neural networks (NN).

Yang *et al.* [14] presented a DL-based stock market SA and prediction method that depends on the combined technique of LSTM and CNN. The NLP technology is utilised for extracting the sentiment characteristics of economic news and social networking content, and a higher-dimension factor space is built by integrating the market data transaction. Rahman *et al.* [15] presented an Annotators' Instruction Assisted Prompt, an innovative assessment prompts intended to reevaluate the classification of FSA for LLMs. Through the combination of complete tasks initially designed for human impressions with the LLMs' prompt architecture, AIAP wants to regulate the comprehension of sentiment over either machine or human clarifications, giving a better and context-related foundation for SA. Smatov *et al.* [16] presented an innovative method for SA, particularly developed for forecasting stock market activities. The author uses complex mathematical modelling methods to improve both the interpretability and precision of the techniques. Existing studies by Kim *et al.* [11], Narayana *et al.* [12], Pandiri *et al.* [13], and Yang *et al.* [14] mainly focus on the sentiment analysis-based stock prediction by combining CNN, LSTM, RSI and NLP models for enhancing trading decisions. Rahman *et al.* [15] and Smatov *et al.* [16] further improve financial sentiment analysis by advanced prompt-based learning and mathematical modelling methods. However, the challenges associated with secure financial data transmission, IoT-based vulnerabilities and adversarial attacks remain insufficiently addressed. Therefore, an integrated IoT enabled adversarial defense architecture for reliable and secure sentiment driven stock market analysis is still needed.

The rapid expansion of information and communication technology (ICT) has transformed financial intelligence systems by facilitating decision-making, processing and real-time data acquisition, through interconnected techniques. Particularly, IoT-enabled financial platforms provide continuous access to various market information, including sentiment-related data, investor interactions and trading activities. Despite, the increasing dependence on AI driven trading systems introduces security challenges, specifically adversarial attacks which manipulates input data and degrade the reliability of the automated investment decisions. Hence, developing adversarial resilient techniques is essential for ensuring trustworthy and secure financial intelligence. Therefore, this study proposes an adversarial-resilient explainable artificial intelligence for sentiment-driven stock trading (ARXAI-SST) architecture. The key contributions are given as follows.

- Design an adversarial attack detection module based on graph neural networks (GNNs).
- Develop a sentiment analysis module using the BiLSTM-Att model.
- Employ the Adam optimiser for hyperparameter tuning.
- Integrate SHAP-based XAI to provide clear insights into the model's predictions.
- Conduct extensive experimental evaluations on benchmark datasets demonstrating superior performance across multiple evaluation metrics.

2. THE PROPOSED METHOD

In this study, the ARXAI-SST architecture follows a structured workflow for explainable sentiment-driven, accurate and secure stock trading, as given in Figure 1. Initially, the adversarial attack detection module preprocesses the input data by feature scaling and RFE for selecting the most relevant features, which are then categorized using GNN to detect the adversarial activities [17]. Next, the sentiment analysis module preprocesses financial text, gets contextual embeddings by FinBERT, and categorizes market sentiment by a BiLSTM-Att model optimized through Adam optimizer. Finally, SHAP is used to interpret the model predictions by finding the key sentiment features which influences the trading decisions.

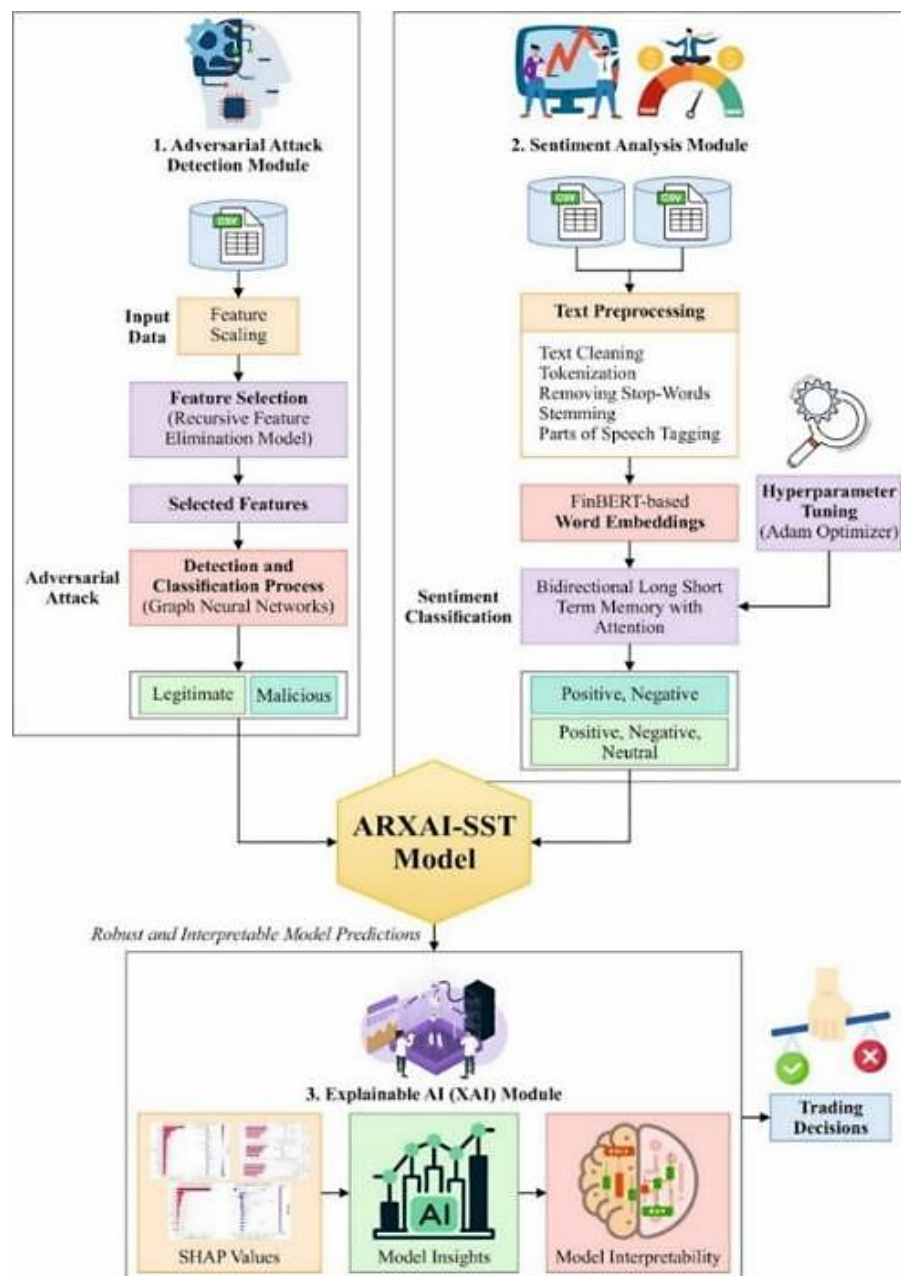


Figure 1. Visual overview of the ARXAI-SST structure

In the proposed architecture, connected digital platforms and IoT enabled financial devices continuously generates communication and transaction data, that was transmitted by the ICT infrastructure to the proposed model. The collected data go through preprocessing, adversarial detection, sentiment analysis,

and prediction for supporting secure financial decision making. Furthermore, the SHAP based explainability module shows transparent interpretations within financial ICT infrastructures. GNN, FinBERT, BiLSTM-Att, and SHAP is selected for explainable and secure financial intelligence. For adversarial attack detection GNN is used, due to its capability of capturing complex relationships over interconnected IoT based trading data. FinBERT is used for sentiment feature extraction as it provides domain specific contextual representations. BiLSTM-Att is used to capture sequential sentiment dependencies. Finally, SHAP is integrated for enhancing model transparency.

The ARXAI-SST architecture is designed for IoT enabled financial environments, where market information, related communications and financial transaction data are continuously created. These heterogeneous data streams are sent through the ICT frame to the proposed model for preprocessing, stock trend prediction, adversarial detection, and sentiment analysis.

2.1. Data preprocessing and feature scaling

The collected datasets were preprocessed for removing inconsistencies, eliminating irrelevant information, and to convert the data into the well-matched formats for the model training. The processed data was then splitted to training and testing phases for the performance assessment. Feature scaling was utilized to ensure that all the input features were changed into a consistent range, which prevents the features with larger values from controlling the learning process.

2.2. Adversarial noise in financial sentiment

Adversarial noise refers to small variations in social media content, reports or financial news that can mislead sentimental classification models without substantially altering the original meaning. The proposed module identifies such varied inputs before sentiment analysis, thus improving the reliability and robustness of the framework.

2.3. Adversarial attack detection module

The adversarial attack detection module is designed to identify malicious activities that may compromise the reliability of sentiment-driven stock trading decisions. Initially, the input data are pre-processed to ensure consistency and improve model training. Recursive feature elimination (RFE) is then utilized to choose the informative attributes by iteratively removing less relevant attributes, thereby reducing redundancy and improving classification performance [18]. The chosen features can be subsequently provided to a GNN for adversarial attack detection. GNN is adopted because it effectively captures structural relationships among interconnected financial data, enabling robust identification of adversarial patterns in graph-based financial networks [19].

2.4. Sentiment analysis module

The SA module evaluates market sentiment from the textual financial data. Initially, the raw text is preprocessed to improve the data quality. FinBERT is then used to generate context word embeddings, which are given as input to a BiLSTM with an attention mechanism for the sentiment classification into positive or negative classes [20]. The attention mechanism highlights the most informative context features, thereby enhancing classification performance. Finally, the model parameters are optimized by the Adam optimizer to achieve high convergence and improved prediction accuracy [21]. Specifically, Algorithm 1 detects adversarial attacks by processing financial dataset D through RFE feature selection, graph construction GNN, and cross-entropy loss optimization to output an attack label, whereas Algorithm 2 performs sentiment analysis on financial text T by extracting contextual features with FinBERT and Attention-based BiLSTM optimized by Adam to output a positive or negative sentiment label. The algorithms for adversarial attack detection module and sentiment analysis module are presented as follow.

Algorithm 1. Adversarial attack detection

Input: Financial dataset D
Output: Adversarial attack label

1. Loading dataset D .
2. Preprocessing D .
3. Selecting informative features using RFE.
4. Constructing graph $G(V, E)$.
5. Training GNN with selected features.
6. Updating model parameters by cross-entropy loss.
7. Predicting attack class.
8. Returning the attack label.

Algorithm 2. Sentiment analysis

Input: Financial text T
Output: Sentiment label

1. Loading text dataset T.
2. Preprocessing text.
3. Generating embeddings using FinBERT.
4. Extracting contextual features by BiLSTM with Attention.
5. Optimizing model using Adam.
6. Predicting Positive or Negative sentiment.
7. Returning sentiment label.

2.5. Model interpretability via SHAP

Due to their restricted interpretability, DL methods are generally described as black boxes. To enhance model transparency, SHAP is employed to evaluate the impact of every feature for the prediction [22]. SHAP assigns a significance value to every feature by evaluating its influence on the model result, enabling the identification of important factors that drive financial sentimental predictions and enhancing the interpretability of the proposed framework.

3. RESULTS AND DISCUSSION

In this section, the empirical validation of the ARXAI-SST technique is inspected utilising three datasets, namely adversarial ML dataset [23], stock-market sentiment dataset [24], and financial sentiment analysis dataset [25]. The technique is executed by using Python 3.6.5 with an i5-8600k CPU, 4 GB GPU, 16 GB RAM, 250 GB SSD, and 1 TB HDD. Table 1 shows the parameter settings of the proposed method.

Table 1. Parameter settings of the ARXAI-SST method

Module	Hyperparameter	Optimal value
FinBERT embedding	Maximum sequence length	256
	Embedding dimension	768
	Dropout rate	0.2
GNN	Number of graph layers	3
	Hidden dimension	128
	Attention heads	4
BiLSTM with attention	BiLSTM layers	2
	Hidden units	128
	Attention heads	4
Training configuration	Dropout rate	0.2
	Optimizer	Adam
	Learning rate	0.001
	Batch size	32
	Epochs	50
	Weight decay	1×10^{-4}
	Early stopping patience	10

3.1. Result analysis of adversarial ml dataset

The experimentation analysis of the ARXAI-SST method is inspected under the adversarial ML dataset [26]-[29]. DNS tunnelling deals with network data gained during a DNS tunnelling attack. The total count of features is 12, and all 12 features were chosen. The dataset encompasses 5999 instances under two classes. Table 2 depicts the comparison assessment of the ARXAI-SST framework with existing systems. The performance outcome showed that the ARXAI-SST model obtains considerable outcomes with $accuracy$ of 97.22%, $precision$ of 95.95%, $recall$ of 97.22%, and $F1_{score}$ of 96.56%, correspondingly. Additionally, the isolation forest (IF) and J48 models get somewhat lesser performance with $accuracy$ of 96.33% and 96.11%, $precision$ of 91.13% and 90.71%, $recall$ of 92.15% and 88.97%, and $F1_{score}$ of 89.89% and 95.32%, respectively.

Figure 2 explains both global and local interpretations of the model employing SHAP values. The global feature significance plot displays that mA is the most powerful feature, contributing significantly more to the model's predictions than the others. Features like mQ , vA , and sA are presented as of reasonable importance, whereas the residual features can have comparatively smaller impacts. The local explanation summarises how individual feature values affect the output variable g across various instances. Positive SHAP values specify an upsurge in the prediction, while negative values show a reduction.

The colour gradient (blue to red) denotes lower to higher feature values, underscoring how dissimilarities in feature magnitude impact the model's behaviour. The SHAP analysis furthermore validates that the model predictions are basically driven by meaningful economic indicators instead of adversarial trigger patterns. The control of economically relevant features and the limited contributions of unrelated features indicate that the model captures market related signals and lowers dependence on feasibly manipulated keywords.

Table 2. Comparison of outcomes of the ARXAI-SST method with existing models on the adversarial ML dataset

Models	$Accur_y$	$Preci_n$	$Recal_l$	$F1_{score}$
IF	96.33	91.13	92.15	89.89
SVM	89.33	84.25	94.59	89.90
J48 model	96.11	90.71	88.97	95.32
Naïve Bayes	92.40	86.20	89.56	92.66
K-means clustering	95.67	84.73	87.06	84.16
Neural Net	81.10	88.55	94.09	85.75
Random forest	82.00	84.20	95.01	91.34
ARXAI-SST	97.22	95.95	97.22	96.56

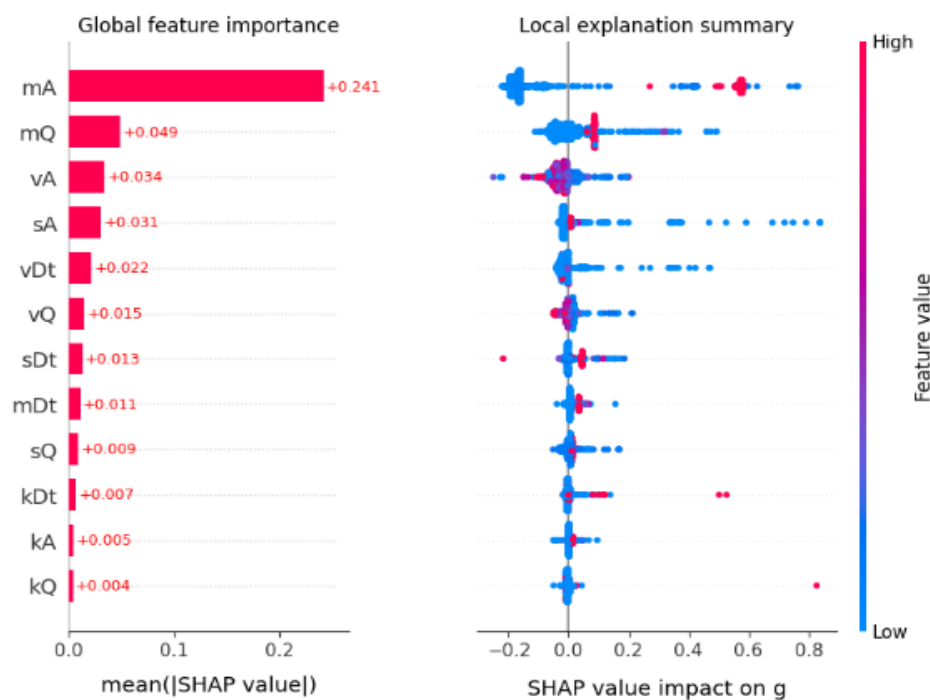


Figure 2. SHAP-based global and local interpretability analysis of adversarial ML dataset

3.2. Result analysis of stock-market sentiment dataset

The empirical assessment of the ARXAI-SST method is achieved under the stock-market sentiment dataset. Gathered stock news from multiple Twitter handles regarded economic news, separating into two parts: negative (-1) and positive (1). The dataset encompasses a total of 5791 counts under negative holds, 2,106, and positive holds, 3,685.

Table 3 illustrates the comparison performance of the proposed framework with existing methods on the stock-market dataset. The SVM, LR, and RF models achieved lower performance, while BERT, FinBERT, GPT-4o, and GPT-4o-mini showed improved results. Unlike the proposed ARXAI-SST method accomplished high performance with 97.74% accuracy, 97.90% precision, 97.74% recall, and 97.82% F1-score. These results demonstrate the efficiency of proposed model in enhancing sentiment driven stock trading decisions.

Table 3. Comparative outcome of ARXAI-SST method with existing models on stock-market dataset

Model	$Accur_y$	$Preci_n$	$Recal_l$	$F1_{score}$
GPT-4o	87.79	87.86	87.79	87.69
GPT-4o-mini	87.79	87.74	87.79	87.73
BERT	81.20	81.50	81.20	81.16
FinBERT	80.04	80.04	80.04	80.04
SVM	64.53	65.68	64.53	64.38
RF model	65.31	65.55	65.31	65.31
Logistic-regression	64.92	65.89	64.92	64.74
ARXAI-SST	97.74	97.90	97.74	97.82

The ablation results using accuracy, precision, recall, and F1-score demonstrate the contribution of each component in ARXAI-SST. Table 4 demonstrates the ablation analysis of the proposed method. For the adversarial ML dataset, ARXAI-SST (Scaling + RFE + GNN) achieves 97.22% accuracy and 96.56% F1-score. For the stock market dataset, the complete model (FinBERT + BiLSTM-Att + Adam) obtains 97.74% accuracy and 97.82% F1-score, while the financial sentiment dataset achieves 97.75% accuracy and 95.26% F1-score. These results confirm that the combination of feature selection, GNN, FinBERT, attention mechanism, and Adam optimizer improves the overall robustness and prediction performance.

Table 4. Ablation study of the ARXAI-SST method

Models	$Accur_y$	$Preci_n$	$Recal_l$	$F1_{score}$
Adversarial ML dataset				
Without the RFE feature selection	95.91	94.65	96.00	95.27
GNN only	96.71	95.15	96.62	95.91
ARXAI-SST (Scaling + RFE + GNN)	97.22	95.95	97.22	96.56
Stock-market dataset				
BiLSTM only (without attention)	95.93	95.96	95.63	95.88
BiLSTM-Att only	96.68	96.49	96.19	96.53
FinBERT + BiLSTM-Att (without Adam optimizer)	97.20	97.20	96.99	97.03
ARXAI-SST (FinBERT + BiLSTM-Att + Adam)	97.74	97.9	97.74	97.82
Financial sentiment analysis dataset				
BiLSTM only (without attention)	95.54	94.52	92.51	93.51
BiLSTM-Att only	96.29	95.08	93.11	94.09
FinBERT + BiLSTM-Att (without Adam optimizer)	96.96	95.75	93.69	94.72
ARXAI-SST (FinBERT + BiLSTM-Att + Adam)	97.75	96.32	94.40	95.26

4. CONCLUSION

In this paper, the ARXAI-SST method is presented as an explainable and secure framework for sentiment driven stock trading decisions in IoT enabled financial environments. The proposed method enables users to understand the justification behind market trend predictions and to verify whether decisions are based on the genuine market behaviour. The proposed method ensures transparent, accurate and robust trading decisions. The experimental assessment on benchmark datasets shows that the proposed framework attains greater performance than the existing systems. Beyond performance improvements, the proposed architecture has substantial potential for real world deployment in fintech platforms. Its explainability capability can also support the regulatory compliance by providing the transparent insights into AI driven trading decisions. Although the proposed framework demonstrates high performance, the experiments were conducted by benchmark datasets, which may not completely capture real world financial market dynamics. In addition, live trading assessments and financial back testing were over the scope of this study. These limitations may impact the evaluation of practical deployment, and the future work will highlight on validation of the architecture in real time IoT enabled financial environments.

FUNDING INFORMATION

The authors received no funding for this study.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Suresh Talamala	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Sukhada Aloni		✓				✓		✓	✓	✓	✓	✓		
J. Vijayalakshmi	✓		✓	✓			✓			✓	✓		✓	
Subham Pankaj		✓			✓		✓	✓		✓	✓	✓	✓	
Samantaray														
K. Swanthana		✓	✓			✓		✓	✓		✓		✓	
Nisarg Gandhewar	✓		✓		✓	✓			✓	✓		✓		

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are openly available in the Kaggle repository at

- <https://www.kaggle.com/datasets/cnrieit/adversarial-machine-learning-dataset>,
- <https://www.kaggle.com/datasets/yash612/stockmarket-sentiment-dataset>, and
- <https://www.kaggle.com/datasets/sbhatti/financial-sentiment-analysis>, reference numbers [23]-[25].

REFERENCES

- [1] E. Cicekyurt and G. Bakal, "Enhancing sentiment analysis in stock market tweets through BERT-based knowledge transfer," *Computational Economics*, vol. 67, no. 2, pp. 855–877, Feb. 2026, doi: 10.1007/s10614-025-10901-8.
- [2] E. Muthukumar, H. P. Josyula, S. K. Gatala, M. K. Vandanapu, V. Mistry, and N. Singh, "AI-driven predictive analytics for financial market forecasting," in *Proceedings of the 2025 International Conference on Technology Enabled Economic Changes, InTech 2025*, IEEE, Feb. 2025, pp. 1389–1394, doi: 10.1109/InTech64186.2025.11198418.
- [3] H. R. B. Seshakagari, A. Umashankar, T. Harikala, L. Jayasree, and J. Severance, "Dynamic financial sentiment analysis and market forecasting through large language models," *International Journal of Human Computations & Intelligence*, 2025, [online]. available: <http://creativecommons.org/licenses/by/4.0/397>
- [4] F. M. P. Fozap, "Hybrid machine learning models for long-term stock market forecasting: integrating technical indicators," *Journal of Risk and Financial Management*, vol. 18, no. 4, p. 201, Apr. 2025, doi: 10.3390/jrfm18040201.
- [5] T. Kumar, "Deep learning-based stock price forecasting for business management: a hybrid approach using LSTM and sentiment analysis," *EKSPLORIUM-BULETIN PUSAT TEKNOLOGI BAHAN GALIAN NUKLIR*, vol. 46, no. 1, pp. 1598–1613, 2025.
- [6] K. Alam, M. H. Bhuiyan, I. Ul Haque, M. F. Monir, and T. Ahmed, "Enhancing stock market prediction: a robust LSTM-DNN model analysis on 26 real-life datasets," *IEEE Access*, vol. 12, pp. 122757–122768, 2024, doi: 10.1109/ACCESS.2024.3434524.
- [7] D. G. Takale, "Enhancing financial sentiment analysis: a deep dive into natural language processing for market prediction industries," *Journal of Computer Networks and Virtualization*, vol. 2, no. 2, pp. 1–5, 2024, doi: 10.48001/jocnv.2024.221-5.
- [8] S. Banoth and S. Yadala, "A hybrid deep learning framework for stock price forecasting with sentiment analysis," in *Proceedings of the 2024 13th International Conference on System Modeling and Advancement in Research Trends, SMART 2024*, IEEE, Dec. 2024, pp. 467–471, doi: 10.1109/SMART63812.2024.10882215.
- [9] V. Khandelwal, H. Varshney, and G. Munjal, "Sentiment analysis based stock price prediction using machine learning," in *Proceedings - 2nd International Conference on Advancement in Computation and Computer Technologies, InCACCT 2024*, IEEE, May 2024, pp. 182–187, doi: 10.1109/InCACCT61598.2024.10551038.
- [10] S. Prabakar, A. Kumar, R. Jayakarthish, D. Venkatesh, R. S. Pratheeba, and B. Khan, "Empirical evaluation of stock market prediction system using intelligent learning scheme with data processing logic," in *Proceedings - 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2024*, IEEE, Mar. 2024, pp. 290–297, doi: 10.1109/ICICV62344.2024.00050.
- [11] Y. Kim, S. Yoo, and S. Park, "A rule-based stock trading recommendation system using sentiment analysis and technical indicators," *Electronics (Switzerland)*, vol. 14, no. 4, p. 773, Feb. 2025, doi: 10.3390/electronics14040773.
- [12] M. L. Narayana, A. J. Kartha, A. K. Mandal, R. P. A. Suresh, and A. C. Jose, "Ensemble time series models for stock price prediction and portfolio optimization with sentiment analysis," *Journal of Intelligent Information Systems*, vol. 63, no. 4, pp. 1079–1103, Aug. 2025, doi: 10.1007/s10844-025-00928-6.
- [13] R. Pandiri, K. Thilagavathi, A. Mittal, M. M. Almusawi, P. Nagaveni, and T. R. Kumar, "Utilizing recurrent neural networks for sentiment analysis of financial news to enhance market prediction and investment strategies," in *2025 International Conference on Automation and Computation, AUTOCOM 2025*, IEEE, Mar. 2025, pp. 285–289, doi: 10.1109/AUTOCOM64127.2025.10957345.
- [14] W. Yang, J. Lin, H. Xue, and J. Wang, "Research on stock market sentiment analysis and prediction method based on convolutional neural network," in *Proceedings of the 2025 International Conference on Machine Learning and Neural Networks, MLNN 2025*, New York, NY, USA: ACM, Apr. 2025, pp. 91–96, doi: 10.1145/3747227.3747241.

- [15] A. M. M. Rahman, A. Uddin, and G. “Grace” Wang, “Evaluating financial sentiment analysis with annotators instruction assisted prompting: enhancing contextual interpretation and stock prediction accuracy,” *arXiv preprint arXiv:2505.07871*, 2025, [Online]. Available: <http://arxiv.org/abs/2505.07871>
- [16] N. Smatov, R. Kalashnikov, and A. Kartbayev, “Development of context-based sentiment classification for intelligent stock market prediction,” *Big Data and Cognitive Computing*, vol. 8, no. 6, p. 51, May 2024, doi: 10.3390/bdcc8060051.
- [17] R. Hasan *et al.*, “Enhancing malware detection with feature selection and scaling techniques using machine learning models,” *Scientific Reports*, vol. 15, no. 1, p. 9122, Mar. 2025, doi: 10.1038/s41598-025-93447-x.
- [18] S. Alkhliwi, “Modelling of hybrid deep learning framework with recursive feature elimination for distributed denial of service attack detection systems,” *Scientific Reports*, vol. 15, no. 1, p. 39261, Nov. 2025, doi: 10.1038/s41598-025-22936-w.
- [19] Y. Wang and X. Liang, “Application of reinforcement learning methods combining graph neural networks and self-attention mechanisms in supply chain route optimization,” *Sensors*, vol. 25, no. 3, p. 955, Feb. 2025, doi: 10.3390/s25030955.
- [20] Z. Tian, D. Chen, and L. Zhao, “Short-term energy consumption prediction of large public buildings combined with data feature engineering and bilstm-attention,” *Applied Sciences (Switzerland)*, vol. 14, no. 5, p. 2137, Mar. 2024, doi: 10.3390/app14052137.
- [21] H. Sun *et al.*, “A gastrointestinal image classification method based on improved adam algorithm,” *Mathematics*, vol. 12, no. 16, p. 2452, Aug. 2024, doi: 10.3390/math12162452.
- [22] M. H. Abdullah and Y. T. Mustafa, “Machine Learning and SHAP-based analysis of deforestation and forest degradation dynamics along the Iraq–Turkey border,” *Earth (Switzerland)*, vol. 6, no. 2, p. 49, Jun. 2025, doi: 10.3390/earth6020049.
- [23] Kaggle, “Adversarial machine learning dataset,” Kaggle. <https://www.kaggle.com/datasets/cnrieit/adversarial-machine-learning-dataset>
- [24] Y. Chaudhary, “Stock-market sentiment dataset,” kaggle. <https://www.kaggle.com/datasets/yash612/stockmarket-sentiment-dataset>
- [25] Sbhatti, “Financial sentiment analysis,” Kaggle. <https://www.kaggle.com/datasets/sbhatti/financial-sentiment-analysis>
- [26] G. De Bernardi, G. B. Gaggero, F. Patrone, S. Zappatore, M. Marchese, and M. Mongelli, “Rule-based eXplainable autoencoder for DNS tunneling detection,” *Computers*, vol. 14, no. 9, p. 375, Sep. 2025, doi: 10.3390/computers14090375.
- [27] D. R. Insua, R. Naveiro, and V. Gallego, “Perspectives on adversarial classification,” *Mathematics*, vol. 8, no. 11, p. 1957, Nov. 2020, doi: 10.3390/math8111957.
- [28] D. K. Nasiopoulos, K. I. Roumeliotis, D. P. Sakas, K. Toudas, and P. Reklitis, “Financial sentiment analysis and classification: a comparative study of fine-tuned deep learning models,” *International Journal of Financial Studies*, vol. 13, no. 2, p. 75, May 2025, doi: 10.3390/ijfs13020075.
- [29] R. Alawaji and A. Aloraini, “Sentiment analysis of digital banking reviews using machine learning and large language models,” *Electronics (Switzerland)*, vol. 14, no. 11, p. 2125, May 2025, doi: 10.3390/electronics14112125.

BIOGRAPHIES OF AUTHORS



Suresh Talamala    is an assistant professor in the School of Business at Aditya University, Surampalem, Kakinada, Andhra Pradesh, India. His academic interests include business analytics, artificial intelligence, financial technologies, and data-driven decision-making. He can be contacted at email: dr.sureshsony@gmail.com.



Sukhada Aloni    is an assistant professor in the Department of Computer Engineering at A. P. Shah Institute of Technology, Thane (West), Maharashtra, India. Her research interests include computer engineering, artificial intelligence, machine learning, and intelligent computing systems. She can be contacted at email: ssaloni@apsit.edu.in.



J. Vijayalakshmi    is an associate professor in the Department of Artificial Intelligence and Data Science at St. Joseph's College of Engineering, Chennai, Tamil Nadu, India. Her research focuses on artificial intelligence, data science, machine learning, and intelligent data analytics. She can be contacted at email: jr.vijiofficial@gmail.com.



Subham Pankaj Samantaray    is an assistant professor in the Department of Computer Science and Engineering at Nigam Institute of Engineering and Technology, Odisha, India. His areas of interest include computer science, machine learning, data analytics, and intelligent computing. He can be contacted at email: jpp42003@yahoo.co.in.



K. Swanthana    is an assistant professor in the Department of Computer Science and Engineering at Koneru Lakshmaiah Education Foundation, Hyderabad, Telangana, India. Her research interests include artificial intelligence, machine learning, data analytics, and software engineering. She can be contacted at email: kswanthana@gmail.com.



Nisarg Gandhewar    is an assistant professor in the Department of Artificial Intelligence and Machine Learning at Ramdeobaba University, Nagpur, Maharashtra, India. His research interests include artificial intelligence, machine learning, deep learning, and intelligent systems. He can be contacted at email: nisarg.gandhewar@gmail.com.