

An explainable AI-based intrusion detection system for cyber threats in stock markets using the SECURE framework

Anandhi Ramani¹, Malathy S.¹, Ramya K.²

¹PG and Research Department of Computer Science, Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai, India

²PG Department of Information Technology and BCA, Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai, India

Article Info

Article history:

Received Feb 2, 2026

Revised Sep 6, 2026

Accepted Sep 18, 2026

Keywords:

Artificial intelligence

Cybersecurity

Explainable AI

Intrusion detection system

Market manipulation

ABSTRACT

As electronic trading technology accelerates the way trades occur in financial markets, the ability to manipulate the markets in many different ways has become stronger through this same technology. Two ways this happens are via spoofing and layering, which pervert the way prices are determined, confuse investors, and reduce the level of trust in the integrity of financial markets. Existing surveillance mechanisms were predominantly rule-based or relied on opaque machine learning models, limiting their adaptability and interpretability. This study proposed SECURE, an explainable artificial intelligence (AI)-based intrusion detection system designed to detect and interpret spoofing and layering activities in real time. The framework integrated ensemble machine learning models, cybersecurity-inspired monitoring logic, and shapley additive explanations (SHAP)-based explainability to achieve accurate detection with transparent decision-making. Using Level-II order book data, the system analysed behavioural and microstructural trading features to classify manipulative patterns while generating feature-level explanations for each alert. Experimental evaluation demonstrated that the proposed framework achieved high detection accuracy, low false-positive rates, and dependable real-time performance. The results indicated that combining intrusion detection principles with explainable AI improved regulatory interpretability and strengthened the effectiveness of automated market surveillance systems.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Anandhi Ramani

PG and Research Department of Computer Science, Dwaraka Doss Goverdhan Doss Vaishnav College

Chennai, Tamil Nadu, India

Email: sekadhi@gmail.com

1. INTRODUCTION

In the list of these cybersecurity threats, some methods of market manipulation like spoofing and layering pose a significant threat to market integrity and investor confidence [1]. In case of spoofing, large buy and sell orders are placed but there is no intention behind them for actual execution of trade while in case of layering, perceived [2] depth of the market is manipulated through placing various orders at varying price levels [3]. Such manipulative techniques distort the process of price discovery and create artificial liquidity within the financial markets. Retail investors can be easily manipulated through these strategies since they mainly use publicly available order book data for their trades [4].

However, the current market surveillance technologies heavily use rule-based and threshold-based approaches for recognizing suspicious behaviors in the market [5]. While such an approach is quite successful when detecting specific violations, it fails to evolve in response to the new and increasingly complex manipulations in the financial market. Additionally, using strict rule-based criteria often leads to a large amount of false positives, causing an increased workload for the regulators and, thus, decreasing the efficiency of automatic market surveillance technologies. Therefore, it was decided to use artificial intelligence (AI) and machine learning algorithms to perform market surveillance.

For dealing with the interpretability issues associated with traditional AI algorithms, the methods of explainable artificial intelligence (XAI) have received considerable interest in the domain of financial surveillance [6]. One such method is SHAP, which explains the contribution of individual features towards the model prediction [7]. Despite the advantages of XAI for making the model more interpretable, previous research does not consider the implementation of explainability along with real-time surveillance and cyber security based intrusion detection system [8].

Driven by such research issues, this paper aims to introduce SECURE, an intrusion detection framework based on cybersecurity concepts for spoofing and layering in stock markets. Xu and Lin [9] This framework utilizes machine learning, structured validation with rules, and XAI for real-time and accurate detection and monitoring in stock markets [10]. By applying behavioral analysis together with explainable decision support tools, SECURE intends to improve transparency in the market, increase regulatory control, and offer better protection for investors. The next section describes past research studies and their limitations [11].

Table 1 presents a comparative summary of representative studies in market manipulation detection. Table 1 shows that significant achievements have been reached in terms of detection of market manipulations using rule-based surveillance, machine learning approaches, cybersecurity-based intrusion detection system techniques, and explainable AI methods. Although many advancements have been made in this field, there is still a lack of research in terms of creating a holistic surveillance framework instead of just focusing on enhancing certain components of the detection framework. The machine learning approach usually performs well in terms of detection but lacks interpretability while the explanation-based methods hardly ever provide real-time operation capability. On the other hand, cybersecurity-based intrusion detection methods have not been used much for behavioural analysis of Level-II order books data.

Table 1. Comparison of existing studies on market manipulation detection

Citations	Focus	Key strength	Key limitation
[12], [13]	Market volatility, trading activity during cyber-attacks	Shows how cyber threats impact financial markets	Does not detect manipulation patterns
[14], [15]	Order book depth, spoofing patterns, fake liquidity	Strong theoretical basis for spoofing and layering	Not real-time operational
[16], [17]	Cancellation bursts, order lifetime, frequency patterns	Detects high-frequency spoofing strategies	Limited interpretability
[18], [19]	Layering depth, order placement imbalance	Strong regulatory relevance for manipulation cases	High computational overhead
[20], [21]	Distribution shifts in order-flow	Novel quantitative method for spoofing detection	Complex to tune, not industry-ready
[22], [23]	HFT order innovations, manipulation behaviours	Clear distinction between legitimate HFT and abuse	No ML or XAI integration
[24], [25]	System vulnerabilities, attack vectors in finance	Strong justification for IDS inclusion	No trading-pattern detection
[26], [27]	Sector-level cybersecurity challenges	Supports cybersecurity-motivated market surveillance	Not focused on trading microstructure
[28], [29]	High-frequency trade sequences	Strong ML foundation for real-time fraud detection	Black-box, lacks explainability
[30], [31]	Price-volume anomalies, manipulation signals	Modern ML approach for manipulation detection	Does not handle spoofing patterns explicitly

Several research limitations are identified from the existing literature review concerning the problem of stock market manipulation detection. The first one is that the traditional rule-based systems have transparent decision process but lack flexibility in adapting to changing spoofing and layering techniques in dynamic markets [21], [22]. Secondly, despite the fact that machine learning and deep learning models have considerably enhanced detection accuracy, the majority of these models remain black-box systems and thus can hardly

be used for conducting investigation and auditing. Thirdly, current XAI research is predominantly aimed at providing explanation after making the predictions and it is seldom incorporated in the market surveillance process. Lastly, while IDS have been proved to be successful in cybersecurity applications, their application for analysing the behaviour of Level-II order book and traders has been barely explored.

2. THE PROPOSED SECURE FRAMEWORK

2.1. Overview of the proposed SECURE framework

In this paper, we introduce the SECURE framework which is a cybersecurity-inspired and an explainable approach to detect spoofing and layering manipulations in the stock market as shown in Figure 1. Jacob-Leal and Hanaki [23] in contrast to traditional approaches for market surveillance, which use either rule-based monitoring only or machine learning alone, SECURE utilizes ensemble machine learning techniques along with behavioral rule validation and state-based intrusion detection, all under one detection framework, together with XAI techniques. SECURE architecture is made up of six interacting layers, namely the surveillance layer, the examination layer, the control layer, the understanding layer, the response layer, and the enhancement layer.



Figure 1. Layers of the SECURE Framework

2.2. Operational workflow of the SECURE framework

The proposed SECURE framework followed a structured six-stage operational pipeline, as illustrated in Figure 2: Surveillance: real-time ingestion of Level-II order book events; Examination: feature computation and preliminary anomaly scoring; Control: rule-based enforcement using predefined behavioural thresholds; Understanding: generation of SHAP-based explanations; Response: dispatch of structured and explainable alerts; Enhancement: continuous learning through validated analyst feedback.

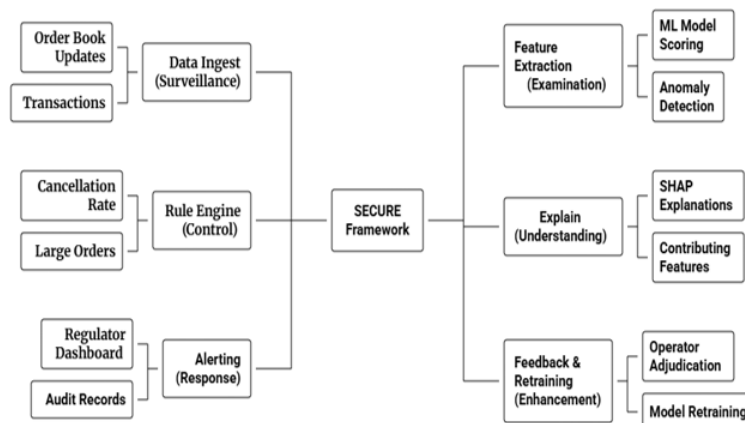


Figure 2. Operational workflow of the SECURE framework

2.3. Explainability mechanism

XAI was implemented using SHAP to generate feature-level attributions [29]. The following is how the explanation function works:

$$f(\mathbf{x}_t) = \phi_0 + \sum_{i=1}^n \phi_i \quad (1)$$

where ϕ_i represents the contribution of the i -th feature to the final model prediction. This formulation enabled transparent interpretation of how individual features influenced the model output.

2.4. Proposed detection models

Three progressively advanced model architectures were implemented.

2.4.1. Model 1: Random forest with SHAP (Baseline)

This baseline model applies supervised learning combined with post-hoc explainability [30].

$$\hat{y}_t = f_{RF}(\mathbf{x}_t) \quad (2)$$

2.4.2. Model 2: SECURE + Random forest + SHAP

This model integrates rule-based evaluation with anomaly scoring [31]. The operational process is described as follows:

$$R_t = g(\mathbf{x}_t) \quad (3)$$

$$A_t = \frac{|\mathbf{x}_t - \mu|}{\sigma} \quad (4)$$

$$S_t = \alpha f_{RF}(\mathbf{x}_t) + \beta A_t + \gamma R_t \quad (5)$$

$$S_t \geq \tau \Rightarrow \text{Suspicious} \quad (6)$$

2.4.3. Model 3: SECURE + Random forest + SHAP + IDS

The final model, algorithm 1 represents the integration of a state-aware intrusion detection system for session-level behavioural correlation [32].

Algorithm 1 IDS-Integrated SECURE Detection

Require: Real-time stream S , IDS engine, RF model

Ensure: Alerts and audit logs

```

1: Initialise IDS session memory
2: for each event  $x_t$  do
3:   Update session state
4:   Extract features
5:   Compute  $R_t$  and  $A_t$ 
6:   Predict RF confidence
7:   Compute IDS correlation score
8:   Compute  $Risk_t$ 
9:   if  $Risk_t$  exceeds thresholds then
10:     Generate SHAP explanation
11:     Create alert and store logs
12:   end if
13: end for
14: Periodically retrain using validated feedback

```

$$C_t = \text{IDS}(\mathbf{x}_t, \mathbf{H}_t) \quad (7)$$

$$Risk_t = w_1 P_t + w_2 A_t + w_3 C_t + w_4 R_t \quad (8)$$

$$Risk_t \geq \tau_{\text{high}} \Rightarrow \text{Critical Alert} \quad (9)$$

$$Risk_t \geq \tau_{\text{med}} \Rightarrow \text{Warning Alert} \quad (10)$$

3. METHOD

3.1. Dataset description

A Level-II stock market order book dataset was employed in this study. Each transaction record contained a timestamp, trading symbol, order price, quantity, order type, execution status, order book depth level, a unique order identifier, volume at the price level, and a derived risk score. The experimental data set contains Level-II stock market order book data with around 800,000 trading instances collected through electronic trading. In this data set, legitimate trading instances are mixed with labelled instances of manipulation, which include spoofing and layering actions. All transactions in the data set have been characterized by market microstructure properties, behavioural measures, and risk properties. The dataset comprised both legitimate trading instances and labelled events reflecting spoofing and layering behaviours [24]. Malicious labels were assigned based on expert-defined behavioural rules derived from prior literature to ensure consistency with realistic market dynamics.

3.2. Dataset availability and reproducibility

Due to regulatory, legal, and confidentiality constraints associated with Level-II stock market data, the raw order book dataset used in this study cannot be publicly released. To address reproducibility concerns, the experimental dataset employed in this study consists of a combination of anonymised real trading records and synthetically generated manipulation samples. The synthetic spoofing and layering events were generated using expert-defined behavioural rules derived from established financial microstructure literature, ensuring that realistic market dynamics and temporal characteristics were preserved. All preprocessing steps, feature engineering procedures, model architectures, and evaluation protocols are fully described within this paper to enable methodological reproducibility. Furthermore, the proposed SECURE framework is model-agnostic and can be applied to any Level-II order book dataset with equivalent feature structure.

3.3. Data preprocessing

Raw trading data were processed to ensure consistency, reliability and suitability for model development [25]. The following preprocessing steps were applied: removal of duplicate and logically inconsistent records, missing value imputation using statistical substitution, Min–Max normalisation of numerical attributes, label encoding of categorical variables, and temporal ordering of transactions to preserve sequence integrity. Formally, each raw record x_t was transformed using a preprocessing function as follows:

$$x_t^* = \mathcal{P}(x_t) \quad (11)$$

where x_t^* represents the cleaned and normalised data instance.

3.4. Feature engineering

After preprocessing, structured features were derived to capture microstructural and behavioural characteristics associated with spoofing and layering [26]. Feature extraction was performed over both short-term and session-based time windows [27]. The feature vector was defined as follows:

$$\mathbf{x}_t = [q_t, p_t, l_t, c_t, b_t, v_t, f_t, r_t, \Delta p_t] \quad (12)$$

where q_t denotes the order size, p_t represents the price relative to the mid-price, l_t corresponds to the order lifetime, c_t indicates the cancellation rate, b_t denotes the order book imbalance, v_t represents the traded volume at the price level, f_t indicates the trader submission frequency, r_t represents the risk score, and Δp_t denotes the short-term price movement.

3.5. Machine learning detection engine

This detection engine uses ensemble tree classifier techniques such as Random Forest and Gradient Boosted Trees due to their resilience to high dimensional structured financial data, as well as SHAP based explainability capability. This technique was trained by the feature vector created from Level-II order book data for classification of trading behavior into either legitimate, spoofing, or layering behavior [28]. The predictive function is formalised as:

$$\hat{y}_t = f_{\text{RF}}(\mathbf{x}_t) \quad (13)$$

where $\hat{y}_t \in \{\text{legitimate, spoofing, layering}\}$.

4. RESULTS AND DISCUSSION

The proposed SECURE framework was evaluated to assess its detection performance and operational feasibility under realistic trading conditions [33]. Three progressively advanced model configurations were implemented: Model 1, Model 2, and Model 3. All models were evaluated using stratified five-fold cross-validation. Performance was measured using accuracy, precision, recall, F1-score, ROC-AUC, false positive rate, detection latency, and memory usage [34].

4.1. Quantitative performance analysis

The Table 2 illustrates evaluation of all models using stratified five-fold cross-validation. Performance was measured using accuracy, precision, recall, F1-score, ROC-AUC, false positive rate, detection latency and memory usage [34].

Table 2. Performance comparison of model configurations

Metric	Model 1	Model 2	Model 3
Accuracy (%)	93.1	95.9	97.0
Precision (%)	78.3	85.1	89.4
Recall (%)	70.0	82.0	87.6
F1-score (%)	73.1	83.6	88.5
ROC-AUC (%)	89.3	93.9	96.2
False positive rate	0.15	0.10	0.06
Latency (ms)	5.4	3.2	1.7
Memory usage (MB)	~100	~140	~210
Real-time capability	No	Partial	Full

4.2. Performance interpretation

Table 2 vividly represents the performance comparison of model configurations whereas the Figure 3 represents the evaluation of models based on their performance. From an operational perspective, these improvements are particularly important: higher precision reduces unnecessary regulatory workload, higher recall reduces the risk of undetected manipulation, and lower false positive rates improve confidence in automated surveillance.

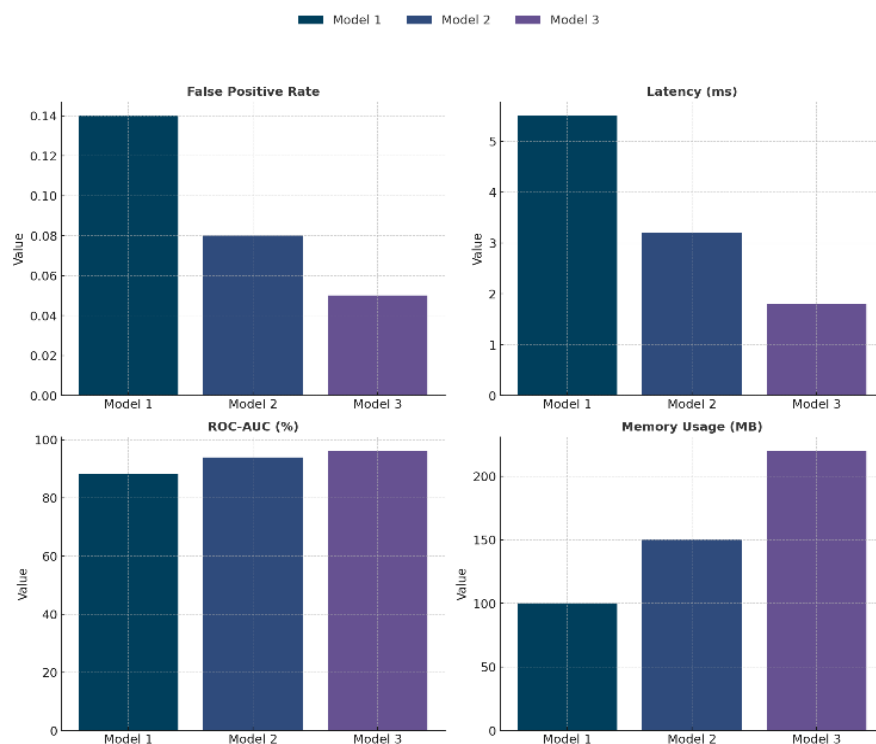


Figure 3. Evaluation of models based on false positive rate, latency, ROC-AUC, and memory usage

4.3. Explainability analysis using SHAP

4.3.1. Global feature importance

An explainability analysis was carried out to determine if the prediction behavior of the framework aligns with what market manipulation experts know about it [35]. Across all model configurations, SHAP analysis consistently identified the most influential behavioural indicators: short-window cancellation rate, relative order size, order book imbalance surveillance, trader submission frequency, and short-term price movement. The strong alignment between SHAP-derived feature rankings and established financial microstructure [36] theory confirms that the model's internal reasoning reflects expert knowledge, which is essential for regulatory acceptance [37].

4.3.2. Local trade-level explanations

At the individual trade level, SHAP explanations indicated that suspicious classifications were primarily driven by: rapid order cancellations, abnormally large order placements, and high-frequency submissions.

4.4. Operational system performance

The full SECURE model generated real-time alerts in under two milliseconds, meeting the operational requirements of exchange-level monitoring [38]. The IDS layer substantially improved alert quality by correlating events across time windows and trader identities, thereby reducing redundant alerts and increasing overall precision. Arifin [39] the feedback-driven enhancement module demonstrated adaptive learning capability. The introduction of a small proportion of analyst-validated feedback resulted in: improved prediction stability, reduced false alert rates, and faster convergence during retraining.

4.5. Comparative analysis among peer system

In contrast to traditional rule-based surveillance systems, which are rigid and prone to alert saturation, SECURE achieves a balanced integration of: adaptability through machine learning, control through rule-based logic, and transparency through SHAP-based explainability.

4.6. Use-case validation

Two representative market scenarios were used to validate practical applicability: a spoofing cluster scenario, in which rapid large-order cancellations were accurately detected and clearly explained [39], and a volatile market layering scenario, where artificial order book depth was successfully identified through IDS-based session correlation [40], [41]. These cases confirm that the framework performs reliably not only in controlled experimental settings but also under realistic market conditions.

5. CONCLUSION

SECURE is the name of the XAI-based intrusion detection system proposed in this paper for detecting and explaining instances of fraudulent behaviors such as spoofing and layering in high-frequency trading financial market environment. The proposed methodology combines the power of machine learning algorithms, cybersecurity-based techniques, and XAI to overcome the drawbacks of traditional rule-based and opaque systems. Experiments conducted show that SECURE provides excellent detection accuracy, low false positive detection rate, and good computational efficiency which allows the framework to be used in the real-time market surveillance system. In addition, the use of SHAP-based explanations helps make the results more interpretable by finding the top important feature contributions in each detection. Due to the implementation of an adaptive feedback loop system, the proposed scheme is able to consistently update its detection approach to counteract newly developed manipulative approaches, thus increasing its stability over time. Future work will involve expanding the scope of SECURE framework to include more types of market manipulations, such as wash trading, front running, and quote stuffing. Future improvements in the framework will also involve integration of multimodal external data sources like financial news and social media sentiments that will enrich context intelligence. Future work will also involve developing the framework with adversarial robustness, increasing computational efficiency to scale up to a bigger size and also using real-world datasets in association with regulatory authorities and stock exchanges to validate the proposed framework.

FUNDING INFORMATION

The authors acknowledge the financial support provided by Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai, through the Research Development Cell and college management, which sanctioned seed funding to support the research activities reported in this study. No external funding agency was involved in this work.

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
Anandhi Ramani	✓	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Malathy S.	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓		
Ramya K.	✓		✓	✓		✓			✓		✓		✓	

C	: Conceptualization	I	: Investigation	Vi	: Visualization
M	: Methodology	R	: Resources	Su	: Supervision
So	: Software	D	: Data Curation	P	: Project Administration
Va	: Validation	O	: Writing - Original Draft	Fu	: Funding Acquisition
Fo	: Formal Analysis	E	: Writing - Review & Editing		

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available upon reasonable request.

REFERENCES

[1] Á. Cartea, S. Jaimungal, and Y. Wang, "Spoofing and price manipulation in order-driven markets," *Applied Mathematical Finance*, vol. 27, no. 1–2, pp. 67–98, Mar. 2020, doi: 10.1080/1350486X.2020.1726783.

[2] G. Mark, "Spoofing and layering," *J Corp L*, vol. 45, no. 2, pp. 399–469, 2020.

[3] J. D. Montgomery, "Spoofing, market manipulation, and the limit-order book," in *SSRN Electronic Journal*, 2016, doi: 10.2139/ssrn.2780579.

[4] B. L. Do and T. J. Putnins, "Detecting layering and spoofing in markets," in *SSRN Electronic Journal*, 2023, pp. 1–58, doi: 10.2139/ssrn.4525036.

[5] J. Tallboys, Y. Zhu, and S. Rajasegarar, "Identification of stock market manipulation with deep learning," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13087 LNAI, 2022, pp. 408–420, doi: 10.1007/978-3-030-95405-5_29.

[6] S. Khodabandehlou and S. A. H. Golpayegani, "Market manipulation detection: a systematic literature review," *Expert Systems with Applications*, vol. 210, p. 118330, Dec. 2022, doi: 10.1016/j.eswa.2022.118330.

[7] Y. Hao, B. Vand, B. M. Delgado, and S. Baldi, "Market manipulation in stock and power markets: a study of indicator-based monitoring and regulatory challenges," *Energies*, vol. 16, no. 4, p. 1894, Feb. 2023, doi: 10.3390/en16041894.

[8] L. N. Mintarya, J. N. M. Halim, C. Angie, S. Achmad, and A. Kurniawan, "Machine learning approaches in stock market prediction: a systematic literature review," *Procedia Computer Science*, vol. 216, no. 4, pp. 96–102, 2023, doi: 10.1016/j.procs.2022.12.115.

[9] J. Xu and J. Lin, "GDet: leveraging graph neural networks for intelligent detection of trade-based market manipulation," in *Proceedings of the 2024 4th International Conference on Big Data, Artificial Intelligence and Risk Management*, New York, NY, USA: ACM, Nov. 2024, pp. 716–723, doi: 10.1145/3718751.3718866.

[10] A. Mashrur, W. Luo, N. A. Zaidi, and A. Robles-Kelly, "Machine learning for financial risk management: A survey," *IEEE Access*, vol. 8, pp. 203203–203223, 2020, doi: 10.1109/ACCESS.2020.3036322.

[11] O. K. Tosun, "Cyber-attacks and stock market activity," *International Review of Financial Analysis*, vol. 76, p. 101795, Jul. 2021, doi: 10.1016/j.irfa.2021.101795.

[12] A. Stenfors, M. Doraghi, C. Soviany, M. Susai, and K. Vakili, "Cross-market spoofing," *Journal of International Financial Markets, Institutions and Money*, vol. 83, p. 101735, Mar. 2023, doi: 10.1016/j.intfin.2023.101735.

[13] X. Tao, A. Day, L. Ling, and S. Drapeau, "On detecting spoofing strategies in high-frequency trading," *Quantitative Finance*, vol. 22, no. 8, pp. 1405–1425, Aug. 2022, doi: 10.1080/14697688.2022.2059390.

- [14] P. Weber, K. V. Carl, and O. Hinz, "Applications of explainable artificial intelligence in finance—a systematic review of finance, information systems, and computer science literature," *Management Review Quarterly*, vol. 74, no. 2, pp. 867–907, Jun. 2024, doi: 10.1007/s11301-023-00320-0.
- [15] T. Tao, C. Zhang, and G. Zhou, "Spoofing detection using wasserstein distance," *Journal of Financial Markets*, vol. 54, no. 100554, 2020, doi: 10.1016/j.finmar.2020.100554.
- [16] V. Dalko and M. H. Wang, "High-frequency trading: order-based innovation or manipulation?," *Journal of Banking Regulation*, vol. 21, no. 4, pp. 289–298, Dec. 2020, doi: 10.1057/s41261-019-00115-y.
- [17] R. Hasan, M. A. Hoque, and M. M. Rahman, "Cybersecurity threats in financial systems," *Computers & Security*, vol. 91, no. 101706, 2020, doi: 10.1016/j.cose.2020.101706.
- [18] F. A. Alzahrani and N. A. E. Alyoubi, "Cybersecurity challenges in the financial sector," *Journal of King Saud University – Computer and Information Sciences*, vol. 34, no. 8, pp. 5381–5392, 2022.
- [19] S. A. Adetoun, "Deep learning vs. real-time financial fraud detection in high-frequency trading," *Journal of Science, Technology and Engineering Research*, vol. 2, no. 4, pp. 28–40, 2024.
- [20] Q. Liu, C. Wang, P. Zhang, and K. Zheng, "Detecting stock market manipulation via machine learning: Evidence from China securities regulatory commission punishment cases," *International Review of Financial Analysis*, vol. 78, p. 101887, Nov. 2021, doi: 10.1016/j.irfa.2021.101887.
- [21] M. E. Verhulst and J. M. E. Pennings, "Spoofing in US futures markets: an interdisciplinary approach," *Capital Markets Law Journal*, vol. 20, no. 3, Jul. 2025, doi: 10.1093/cmlj/kmaf012.
- [22] C. Desagre, F. Laly, and M. Petitjean, "Revisiting the trading activity of high-frequency trading firms around ultra-fast flash events," *Financial Innovation*, vol. 11, no. 1, p. 68, Jan. 2025, doi: 10.1186/s40854-024-00726-z.
- [23] S. Jacob-Leal and N. Hanaki, "Algorithmic trading, what if it is just an illusion? Evidence from experimental asset markets," *Journal of Behavioral and Experimental Economics*, vol. 112, p. 102240, Oct. 2024, doi: 10.1016/j.socec.2024.102240.
- [24] A. Indriawan and N. A. Rakhmawati, "Detecting Manipulation in NFT market using graph-based deep learning," *ECTI Transactions on Computer and Information Technology (ECTI-CIT)*, vol. 19, no. 4, pp. 707–719, Oct. 2025, doi: 10.37936/ecti-cit.2025194.259882.
- [25] A. Alfajeer, A. Altaweel, A. Bouridane, D. Mouheb, and S. Aslam, "On detecting stock price manipulation attacks: a comprehensive systematic literature review," *Multimedia Tools and Applications*, vol. 84, no. 29, pp. 35793–35870, 2025, doi: 10.1007/s11042-025-20641-4.
- [26] K. Lin and Y. Gao, "Model interpretability of financial fraud detection by group SHAP," *Expert Systems with Applications*, vol. 210, p. 118354, Dec. 2022, doi: 10.1016/j.eswa.2022.118354.
- [27] Y. Zhou, H. Li, Z. Xiao, and J. Qiu, "A user-centered explainable artificial intelligence approach for financial fraud detection," *Finance Research Letters*, vol. 58, p. 103479, 2023, doi: 10.1016/j.frl.2023.104309.
- [28] D. Vijayanand and G. S. Smrithy, "Explainable AI - enhanced ensemble learning for financial fraud detection in mobile money transactions," *Intelligent Decision Technologies*, vol. 19, no. 1, pp. 52–67, Jan. 2025, doi: 10.1177/18724981241289751.
- [29] A. Adadi and M. Berrada, "Peeking inside the black-box: a survey on explainable artificial Intelligence (XAI)," *IEEE Access*, vol. 6, pp. 52138–52160, 2018, doi: 10.1109/ACCESS.2018.2870052.
- [30] J. Jin and Y. Zhang, "The analysis of fraud detection in financial market under machine learning," *Scientific Reports*, vol. 15, no. 1, p. 29959, Aug. 2025, doi: 10.1038/s41598-025-15783-2.
- [31] T. Awosika, R. M. Shukla, and B. Pranggono, "Transparency and privacy: the role of explainable AI and federated learning in financial fraud detection," *IEEE Access*, vol. 12, pp. 64551–64560, 2024, doi: 10.1109/ACCESS.2024.3394528.
- [32] S. K. Aljunaid, S. J. Almheiri, H. Dawood, and M. A. Khan, "Secure and transparent banking: explainable AI-driven federated learning model for financial fraud detection," *Journal of Risk and Financial Management*, vol. 18, no. 4, p. 179, Mar. 2025, doi: 10.3390/jrfm18040179.
- [33] S. Latha et al., "An XAI-powered approach for financial fraud detection using anomaly detection and classification techniques," *Journal of Information Systems Engineering and Management*, vol. 2025, no. 55s, pp. 2468–4376, 2024, [Online]. Available: <https://www.jisem-journal.com/>
- [34] M. Muksalmina, A. Syahyana, F. Hidayatullah, G. M. Idroes, and T. R. Noviandy, "Credit card fraud detection through explainable artificial intelligence for managerial oversight," *Indatu Journal of Management and Accounting*, vol. 3, no. 1, pp. 17–28, Jun. 2025, doi: 10.60084/ijma.v3i1.301.
- [35] X. Q. Chen, C. Q. Ma, Y. S. Ren, Y. T. Lei, N. Q. A. Huynh, and S. Narayan, "Explainable artificial intelligence in finance: a bibliometric review," *Finance Research Letters*, vol. 56, p. 104145, Sep. 2023, doi: 10.1016/j.frl.2023.104145.
- [36] A. A. Almazroi and N. Ayub, "Online payment fraud detection model using machine learning techniques," *IEEE Access*, vol. 11, pp. 137188–137203, 2023, doi: 10.1109/ACCESS.2023.3339226.
- [37] J. Černevičienė and A. Kabašinskas, "Explainable artificial intelligence (XAI) in finance: a systematic literature review," *Artificial Intelligence Review*, vol. 57, no. 8, p. 216, Jul. 2024, doi: 10.1007/s10462-024-10854-8.
- [38] P. Dini, A. Elhanashi, A. Begni, S. Saponara, Q. Zheng, and K. Gasmi, "Overview on Intrusion detection systems design exploiting machine learning for networking cybersecurity," *Applied Sciences*, vol. 13, no. 13, p. 7507, Jun. 2023, doi: 10.3390/app13137507.
- [39] M. M. Arifin, "OLGBM: optuna-optimized light gradient boosting machine for intrusion detection," in *Proc. IC4ME2, IEEE*, 2021.
- [40] M. A. Talukder et al., "Machine learning-based network intrusion detection for big and imbalanced data," *Journal of Big Data*, vol. 11, p. 33, 2024, [Online]. Available: <https://doi.org/10.1186/s40537-024-00886-w>
- [41] D. Dalgade, N. Patil, M. Joshi, and D. Hiran, "Enhancing WSN intrusion detection: two-tier feature selection and optuna-optimized ensemble learning," *International Journal of Wireless & Mobile Networks*, vol. 17, no. 1, May 2025, doi: 10.21203/rs.3.rs-6726618/v1.

BIOGRAPHIES OF AUTHORS

Dr. Anandhi Ramani    is an academician in the field of computer applications with a strong focus on teaching, curriculum development, and research-oriented learning. She has been actively involved in designing outcome-based curricula, mentoring students, and integrating emerging technologies such as cloud computing, serverless computing, cybersecurity, and data-driven applications into academic programs. Her academic interests include improving pedagogical practices for diverse learners, guiding student projects, and contributing to research publications and quality assurance activities in higher education. She can be contacted at email: sekadhi@gmail.com.



Malathy S.    is a full-time Ph.D. research scholar in the PG and Research Department of Computer Science at Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai, Tamil Nadu, India. She holds a master's degree in Computer Applications and has qualified the UGC-NET examination in Computer Science and Applications. Her research interests include cybersecurity, stock market manipulation detection, explainable artificial intelligence, intrusion detection systems, and financial data analytics. She can be contacted at email: malathy10112001@gmail.com.



Ramya K.    is a faculty member in the field of computer science with a strong focus on software engineering and system modeling. Her research interests include Unified Modeling Language, software design methodologies, and the integration of emerging technologies in education and organizational systems. She actively engages in scholarly research, academic writing, and conference-oriented studies to enhance both theoretical and practical knowledge. She participates in faculty development and induction programs to strengthen her research and pedagogical competencies. Her academic goal is to contribute high-quality research that supports innovation, effective teaching, and knowledge dissemination. She can be contacted at email: ramya.dgvc2024@gmail.com.