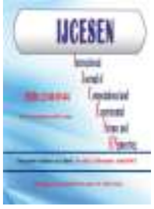
International Journal of Computational and Experimental Science and ENgineering
(IJCESEN)

Vol. 11-No.2 (2025) pp. 3215-3224
http://www.ijcesen.com

ISSN: 2149-9144

Research Article



Secure Optimization of API-Driven Financial Transactions Using Deep Learning: A Threat Detection Framework for Mutual Fund Processing

Jaya Krishna Modadugu*

Software Engineer, Prosper Marketplace Inc, California, USA
* **Corresponding Author Email:** jayakrishna.modadugu@gmail.com- **ORCID:** 0009-0008-9086-6145

Article Info:

DOI: 10.22399/ijcesen.2291
Received : 28 February 2025
Accepted : 13 May 2025

Keywords :

Application Programming Interfaces,
Financial Transactions,
Detection, Mutual Fund Processing,
Intrusion Attempts,
Data Exfiltration,
Unauthorized API Access.

Abstract:

For software applications and systems to interact smoothly and support automated and efficient service delivery, system-to-system communication via Application Programming Interfaces (APIs) is crucial. APIs enable the sharing of data and functions across various platforms, improving both operational performance and user interaction. However, this integration can expose systems to security threats that may be exploited by malicious entities, emphasizing the need to recognize and address related security risks. In this paper, secure optimization of API-driven financial transactions using deep learning a threat detection framework for mutual fund processing (SO-APID-FT-DL-TDF-MFP) is proposed. At first, the input data is taken from the CIC-IDS2017 dataset. Then, the gathered data are fed into the pre-processing segment using implicit unscented particle filter (IUPF) which is used to eliminating noise. The pre-processed data are fed into Gegenbauer graph neural networks (GGNN) for prediction purpose. GGNN is used to predict potential security threats in the API-driven financial transactions by identifying irregular patterns and anomalies in the transaction data, thereby enhancing the overall security of the mutual fund processing system. Then, the proposed method implemented in python and the performance metrics like accuracy, precision, F1-score, recall, receiver operating characteristic (ROC) and specificity analyzed. The proposed SO-APID-FT-DL-TDF-MFP achieves 98% precision, 97% recall, 96% F1-score, 97.1% specificity, 97.5% accuracy, and 1.149 seconds computational time, with a high ROC of 0.99 compared with existing methods, such as adoption of deep-learning models for managing threat in API calls with transparency obligation practice for overall resilience (MT-APIC-TOP-OR-DL), deep learning for intelligent assessment of financial investment risk prediction (IA-FIRP-DL) and fraud prediction using machine learning: the case of investment advisors in canada (FP-CIAC-ML).

1. Introduction

The financial services industry is undergoing a digital transformation, with API-driven systems emerging as the foundation for seamless, real-time communication between financial institutions, fintech providers, and third-party services [1]. Mutual fund processing, in particular, benefits significantly from APIs, which facilitate faster order placements, streamlined settlements, improved regulatory reporting, and enhanced client engagement [2]. With the global API economy projected to grow at over 32.5% CAGR and reach USD 3034 million by 2028, APIs are becoming essential for modernizing legacy systems and achieving scalable, cost-effective integration [3]. Open banking regulations and the need for transparent, agile infrastructure have further accelerated API adoption in asset management and mutual fund transactions.

However, the widespread adoption of APIs has introduced a host of new challenges—most notably, concerns around data security, privacy, and system integrity [4]. The open and interconnected nature of APIs makes them vulnerable to cyber threats such as data breaches, injection attacks, API hijacking, and denial-of-service attempts. Recent statistics indicate a 400% surge in API-related security breaches, with nearly 90% of financial institutions reporting at least one API-specific vulnerability [5]. Moreover, the complexity of mutual fund transactions, involving multiple systems and stakeholders, amplifies the risk of unauthorized access, data leakage, and regulatory non-compliance. Compounding this is the growing demand for explainable AI models, as regulatory frameworks like the EU AI Act call for transparency in algorithmic decision-making and data usage [6].

This study explores a systematic method to enhancing the security and efficiency of API-driven financial transactions within the mutual fund domain [7]. By focusing on detecting and mitigating cyber threats across data exchange layers, the research emphasizes the importance of intelligent data preprocessing and advanced deep learning for effective anomaly detection [8]. A custom neural architecture is integrated into the framework to ensure accurate threat identification while supporting transparent and interpretable outputs, aligning with modern compliance standards [9]. The proposed model is benchmarked against traditional deep learning approaches to demonstrate improvements in both detection performance and the explainability of results. The overall objective is to establish a robust, scalable, and secure data flow system that meets the evolving demands of financial services while safeguarding sensitive transactional data [10].

2. Literature survey

Various research works were already existed in the literature which depended on API-driven financial transactions using deep learning. Some of them works were inspected here.

N Basheer et al. [11] have suggested a combined architecture that combines deep learning models like MLP and ANN, to detect threats from large API call datasets in system-to-system communication. It addresses challenges like evolving vulnerabilities and high traffic volumes by utilizing security catalogs like CWE and CAPEC, and applying controls from NIST SP 800-53. The study also introduces transparency practices across the AI lifecycle, including SHAP analysis, to enhance model interpretability and provide actionable mitigations for improving system security and resilience. However, disadvantages include high computational costs, model training complexity, potential overfitting, and challenges in real-time threat detection.

Y. Sun and J. Li [12] have addressed the role of financial investment in promoting economic growth, particularly in the information technology sector, and its broader socio-economic benefits. They emphasized the growing complexity of financial risks and the necessity for a scientifically-based early warning system to address systemic financial risks. The study innovatively applied deep learning to reconstruct the financial security evaluation and early warning index system, offering valuable support for regulatory authorities. However, the approach may face challenges likedata quality issues, overfitting, the need for extensive computational resources, and difficulties in model interpretability for practical implementation.

M. E. Lokanan and K. Sharma [13] have developed machine learning models with an emphasis on investment fraud to identify fraud in Canada's financial markets. They used data from 406 tribunal cases (2008-2019) provided by the investment industry regulatory organization of Canada (IIROC). Key features, such as investment amounts and offenders' links to bank-owned firms, were identified to predict fraud. The study provided valuable insights for regulators and managers, though its reliance on past data may limit real-time fraud detection and adaptation to emerging fraud schemes.

A. K. Bayya [14] had examined API security challenges in the FinTech sector, emphasizing adaptive security models and Zero Trust Architecture (ZTA) for securing APIs, which were crucial for digital transformation in financial services. The study addressed threats such as unauthorized access, data breaches, and fraud, proposing strategies like dynamic authentication, encryption, and AI-driven threat detection, along with ZTA’s "never trust, always verify" principle. It also considered regulatory requirements like GDPR, PCI DSS, and PSD2. However, ZTA's complexity, high implementation costs, and potential performance degradation in real-time systems were noted as drawbacks.

E Brown and M Johnson [15] have suggested APIs have rapidly transformed the fintech sector by enabling seamless data access, integration, and innovation. They promote the development of new financial products and services by enabling safe data exchange between banks, clients, and outside providers. To ensure the security of sensitive financial data, open banking, secure API practices, and data protection frameworks were essential. However, there was security and privacy risks associated with increased accessibility, so strong measures were required to guard against potential breaches or misuse of data. Table 1 presents the literature survey’s summary. Despite the increasing adoption of API-driven platforms in financial services, especially for mutual fund processing, current approaches exhibit several critical drawbacks. Generally, existing systems lack comprehensive and intelligent

Table 1. *Literature survey's summary.*

Ref	Algorithms	Dataset	Advantages	Disadvantages
N Basheer *et al.* [11]	Artificial Neural Network (ANN)	Windows PE Malware API Dataset	Enhances system security and transparency	High computational costs
Y. Sun and J. Li [12]	Recurrent Neural Network (RNN)	**Financial Stability Board (FSB) Dataset**	Enhances risk detection	Data quality concerns
M. E. Lokanan and K. Sharma [13]	Convolutional Neural Network (CNN)	Canadian Securities Administrators (CSA) Dataset	Enhances fraud detection predictions	Relies on past data
A. K. Bayya [14]	Machine Learning (ML)	API Security Vulnerability Datasets	Enhanced security and adaptive models	High implementation costs
E Brown and M Johnson [15]	Convolutional Neural Network (CNN)	Windows PE Malware API Dataset	Improved financial services	Security risks and privacy concerns

frameworks that address the dynamic and high-frequency nature of API-based transactions, resulting in vulnerabilities to sophisticated cyber threats. Many security models focus on broader organizational or national financial risks, overlooking the transactional-level intricacies essential for safeguarding APIs. Methodologically, while deep learning techniques and machine learning have been employed to detect fraud and assess financial risks, they often rely on static data, lack adaptability to real-time API threats, and perform inadequately when faced with irregular or noisy transaction patterns. Traditional models like ANN, RNN, and CNN struggle with precision and consistency in such environments. Furthermore, a major shortcoming is the absence of explainability in most models, which is crucial for regulatory compliance and operational transparency. There is also limited emphasis on advanced preprocessing to filter noise and enhance feature clarity, which is vital for robust threat detection. These shortcomings underscore the need for a more specialized, intelligent, and interpretable approach tailored to the challenges of API-level security. Motivated by these limitations, this research proposes a novel framework to optimize API-driven financial transactions, ensuring secure, transparent, and efficient mutual fund processing.

In this paper, SO-APID-FT-DL-TDF-MFP method addresses the security challenges faced by existing approaches in detecting threats in API-driven financial transactions. This technique enhances the security of mutual fund processing by utilizing IUPF for data pre-processing, which helps reduce noise. The use of GGNN enables accurate threat prediction by identifying complex anomalies and irregularities in transaction data. The GGNN is optimized for improved performance through advanced deep learning techniques, which enhance prediction precision. The SO-APID-FT-DL-TDF-MFP method outperforms existing methods in API-driven financial threat detection, achieving high precision, recall, F1-score, and ROC metrics, while also ensuring faster computational times and reducing false positives.

Important contribution of this work is abridged below,

- In this paper, secure optimization of API-driven financial transactions through deep learning: a threat detection framework for mutual fund processing (SO-APID-FT-DL-TDF-MFP) is proposed.
- Predicting security threats for API-driven financial transactions presents an advanced approach to enhance system security.
- By focusing on mutual fund processing, the study addresses critical security needs in high-value financial transactions, making the framework highly relevant for securing financial systems.
- The framework's ability to predict potential security threats before they fully materialize allows for proactive risk management, preventing potential fraud and breaches in API-driven financial systems.
- The obtained results of proposed SO-APID-FT-DL-TDF-MFP algorithm is comparing to the existing models such as MT-APIC-TOP-OR-DL, IA-FIRP-DL and FP-CIAC-ML respectively.

The remaining manuscript is arranged as follows: Part 2 displays proposed methodology, Part 3 displays the results and Part 5 conclusion the paper.

2. Proposed Methodology

In this sector, secure optimization of API-driven financial transactions using deep learning a threat detection framework for mutual fund processing (SO-APID-FT-DL-TDF-MFP) is discussed. The approach begins with data sourced from the CIC-IDS2017 dataset, which is pre-processed using an implicit unscented particle filter (IUPF) to eliminating noise. The enhanced data is then fed into Gegenbauer Graph Neural Networks (GGNN) for threat prediction. GGNN identifies irregular patterns and anomalies in the transaction data, enabling the detection of potential security threats. This method strengthens the security of API-driven financial transactions, particularly in the context of mutual fund processing systems. Fig 1 displays the block Diagram of the proposed SO-APID-FT-DL-TDF-MFP.

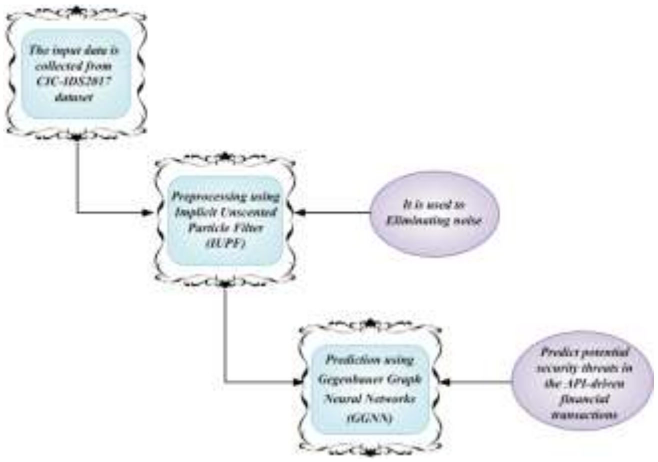

The input data is collected from CIC-IDS2017 dataset
Preprocessing using Implicit Unscented Particle Filter (IUPF)
It is used to Eliminating noise
Prediction using Gegenbauer Graph Neural Networks (GGNN)
Predict potential security threats in the API-driven financial transactions

Figure 1. *Block Diagram of the proposed SO-APID-FT-DL-TDF-MFP*

2.1 Overview of Financial Market Dynamics

The financial market is a vast, multi-level network where various submarkets interact and influence one another. It acts as the center of the economy, directing the movement of money and making it easier to finance it. Financial instruments like credit are used in transactions between fund suppliers and demanders in the financial markets to move money from sectors with excess supply to those in need. In essence, the dynamics and mechanisms of supply and demand created by the exchange of financial assets are represented by a financial market. Based on the length of time that financial transactions take place, one of the most popular ways to categorize financial markets is to separate them into money markets and capital markets. These markets can then be further separated into niche markets that serve various financial products and objectives, all of which support the economy's overall operation.

2.2 Data Acquisition

The input data is initially gathered from the representative CIC-IDS2017 dataset [16], developed by the Canadian institute for cybersecurity. This dataset is widely used to evaluate IoT security frameworks, particularly for intrusion detection with deep learning. It contains a diverse range of labeled attack vectors and benign network traffic relevant to API-based environments. Collected in 2017, the dataset includes various attack types pertinent to IoT. Originally containing 2.8 million instances, the data was pre-processed to refine it to 56,662 records by removing duplicates, handling missing entries, and eliminating irrelevant labels. Training uses 70% of the dataset, testing uses 15%, and validation uses 15%.

2.3 Pre-processing using Implicit Unscented Particle Filter (IUPF)

In this segment, pre-processing using an IUPF [17] is discussed. IUPF is used to eliminating noise. IUPF operates by dynamically filtering local data segments, increasing the accuracy of downstream learning models in handling volatile API communication patterns. The IUPF can be applied to secure optimization in API-driven financial transactions by enhancing the accuracy of threat detection models. Its ability to provide precise state estimates ensures better detection of anomalies in financial data. However, IUPF’s high computational cost, especially in large-scale systems, and the need for careful tuning, can present challenges when applied to the dynamic nature of mutual fund processing and financial data analysis.

The IUPF method is particularly valuable in securing optimization for API-driven financial transactions by refining the accuracy of threat detection models. IUPF is eliminating noise in Equation (1),

$$X_l = j(Y_l) + B_l \tag{1}$$

Here, X_l represents measured at moment l; $j(Y_l)$ denotes the measurement Equation; B_l represents the data during measurement. IUPF's precise state estimation capabilities allow for better identification of anomalies within financial data, which is crucial for detecting potential threats in IUPF method is expressed in Equation (2),

$$res^{l}_{j,m} = \left| f^{l}_{j} = f^{l}_{j,m} \right| \tag{2}$$

Where, $res^{l}_{j,m}$ denotes the residual difference value; f^{l}_{j} is the recorded Euclidean distance between the j^{th} beacon node, $f^{l}_{j,m}$ represents the residual difference value. The IUPF method requires careful tuning to adapt to the dynamic nature of mutual fund processing and financial data analysis expressed in Equation (3),

$$B_j(l) = \sum\nolimits_{m=1}^{M} e^{l}_{m} \cdot f^{l}_{j,m} \tag{3}$$

Here, from the j^{th} BN represents time l, $B_j(l)$ is the weighted average distance; e^{l}_{m} denotes the particle weight, which is its reciprocal; $f^{l}_{j,m}$ denotes the current lateral. Finally, the IUPF method has eliminated noise. The pre-processed data is then used to make predictions.

2.4 Prediction Using Gegenbauer Graph Neural Networks (GGNN)

In this sector, prediction utilizing Gegenbauer graph neural networks (GGNN) [18] is discussed. GGNN is used to predict potential security threats in the API-driven financial transactions by identifying irregular patterns and anomalies in the transaction data, thereby enhancing the overall security of the mutual fund processing system. GGNN can be applied to the secure optimization of API-driven financial transactions by modeling complex relationships within transaction data. GGNN captures nonlinear dependencies between transaction features, ensuring effective threat detection. This method enhances the reliability and security of financial systems, ensuring that mutual fund processing remains secure by leveraging the ability of GGNN to handle graph-structured data, optimizing both performance and protection is expressed in Equation (4),

$$z = v_{\beta}(z)y = xv_{\beta}(\Delta)x^{v}y \tag{4}$$

Where z is represents the Kronecker delta, here v_{β} is represents the spectral domain, and $(z)y$ is represents the initial random variable. xv_{β} is represents the term that takes the temporal dependence of the data, and $x^{v}y$ is represents the consideration throughout the reconstruction procedure. GGNN predicts security threats in API-driven financial transactions by detecting irregular patterns and anomalies, boosting the security of mutual fund processing systems are expressed in Equation (5),

$$v_{\beta}(x) = x^{(1/2)}_{v}(y) \tag{5}$$

Where v_{β} is represents the basis, they may formulate a polynomial sorting function and (x) is represents the wavelength convolutional implementing the normalized laplacian matrix and Gegenbauer polynomials basis for graphs, here $x^{(1/2)}_{v}$ is represents the Gegenbauer polynomials with the help of the subsequent recurrence relationship. GGNN is optimizing the security of mutual fund processing systems, as it can detect any suspicious activities or fraudulent patterns that may otherwise go unnoticed in Equation (6),

$$v_{\beta}(z) = \sum_{x=0}^{\lambda-1} \beta_{x} v_{\partial}(\hat{z}) v_{\beta} v_{\partial}(\hat{z}) \tag{6}$$

Where $v_{\beta}(z)$ is represents the vector of Gegenbauer coefficients for layer, and $\sum_{x=0}^{\lambda-1}\beta_{x}$ is represents the matrix of trainable parameters for layer. Here $(\hat{z})$ is represents the mutual funds and $v_{\partial}(\hat{z})$ is represents security threats. Finally, GGNN predicted security threats in API-driven financial transactions by detecting irregular patterns and anomalies, boosting the security of mutual fund processing systems.

3. Result

The results of proposed technique are discussed in this sector. The proposed SO-APID-FT-DL-TDF-MFP technique is then simulated in Python and compiled employing Jupiter notebook and executed in 64 GB RAM, Intel Core I9-13900k CPU, and 500 GB SSD storage. The process begins by splitting the dataset into training (60%) and testing (40%) sets, followed by performance evaluation of various classification algorithms. The obtained outcome of the proposed SO-APID-FT-DL-TDF-MFP approach is analysed with existing systems like MT-APIC-TOP-OR-DL, IA-FIRP-DL and FP-CIAC-ML respectively.

3.1 Performance Measure

This is an important step in selecting the best classifier. Accuracy, precision, recall, F1-score, and detection rate are among the performance metrics that are evaluated. The performance metric is used to scale the performance metrics. To scale the performance metric, the True Negative , True Positive False Negative and False Positive samples are needed.

3.1.1 Precision

One measure of machine learning method's efficiency is precision, or how well method creates positive forecasts. It is measured using the equation (20) that follows.

$$\Pr ecision = \frac{TP}{(TP + FP)} \qquad (7)$$

3.1.2 Recall

A model's recall quantifies its capacity to accurately detect every pertinent instance, with an emphasis on reducing false negatives. It is crucial in situations where capturing all true positives is more important than avoiding false positives.

$$\text{Re}call = \frac{TP}{TP + FN} \qquad (8)$$

3.1.3 Receiver Operating Characteristic (ROC)

The ROC curve assesses a classifier’s efficacy by plotting the TPR against the FPR, illustrating its ability to distinguish between classes at various thresholds.

$$TPR = \frac{TP}{TP + FN} \qquad (9)$$

3.2 Performance Analysis

Fig 2-6 depicts the simulation outcomes of proposed SO-APID-FT-DL-TDF-MFP method. Then, the proposed SO-APID-FT-DL-TDF-MFP method is likened with MT-APIC-TOP-OR-DL, IA-FIRP-DL and FP-CIAC-ML methods respectively. Fig 2 displays performance analysis of precision.

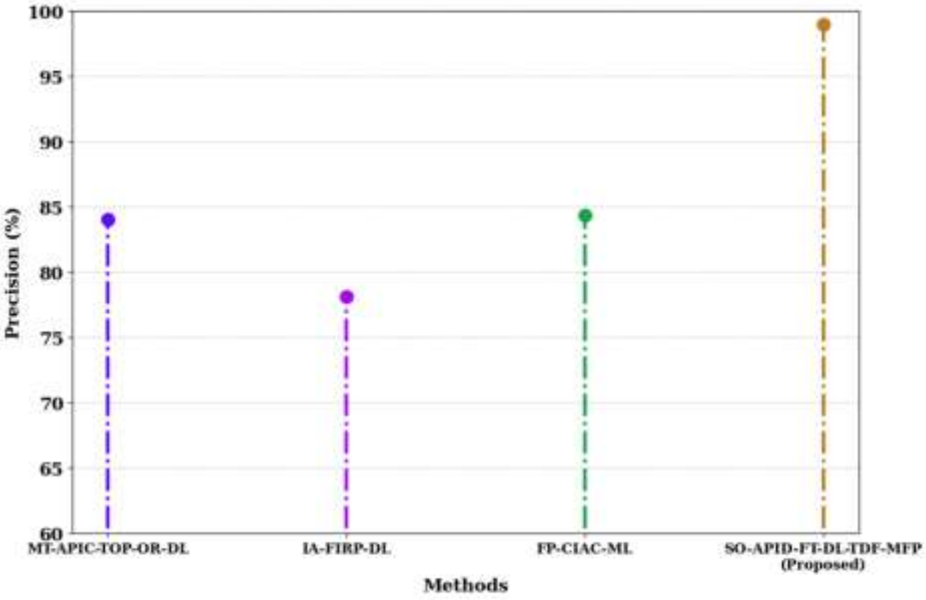


Figure 2. Performance Analysis of Precision

Figure 2 presents a performance analysis of precision in API-driven financial transactions for mutual fund processing, comparing the effectiveness of a deep learning-based threat detection framework in identifying fraudulent activities. MT-APIC-TOP-OR-DL achieves approximately 84% precision, IA-FIRP-DL around 78%, and FP-CIAC-ML about 85%. The proposed method, SO-APID-FT-DL-TDF-MFP, significantly outperforms the others with a precision of approximately 98%. This graph visually highlights the superior performance of the proposed approach, demonstrating its efficiency in ensuring secure and reliable financial transactions.

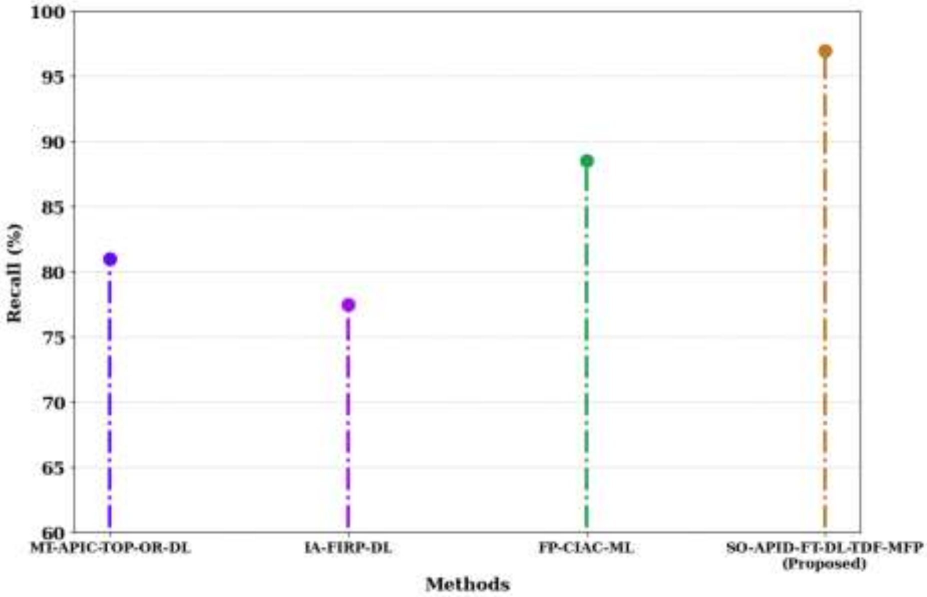


Figure 3. *Performance Analysis of Recall*

Figure 3 illustrates the performance analysis of recall for API-driven financial transactions using deep learning. The graph highlights the effectiveness of a threat detection framework tailored for mutual fund processing, emphasizing how deep learning models improve recall rates in identifying fraudulent or suspicious transactions within financial APIs. The proposed method, SO-APID-FT-DL-TDF-MFP, achieves the highest recall at approximately 97%, demonstrating its superior performance in retrieving relevant instances. FP-CIAC-ML ranks second with a recall of around 88%, while MT-APIC-TOP-OR-DL and IA-FIRP-DL show lower recall values of approximately 81% and 77%, respectively.

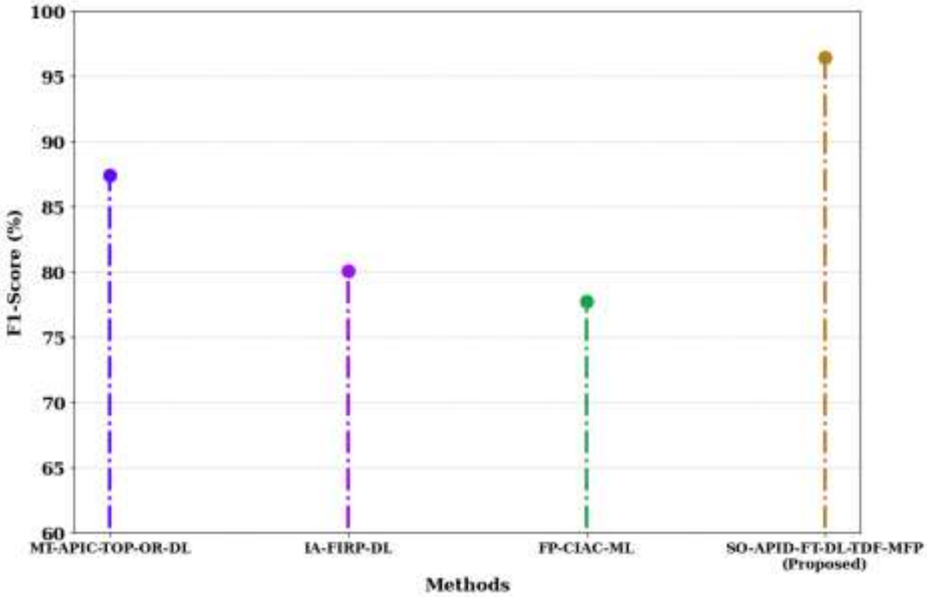


Figure 4. *Performance Analysis of F1-score*

Figure 4 illustrates the performance analysis of the F1-score for API-driven financial transactions, utilizing deep learning in a threat detection framework for mutual fund processing. The graph highlights the accuracy and efficiency of various models in identifying potential threats. MT-APIC-

TOP-OR-DL achieves approximately 87.5%, IA-FIRP-DL around 80%, FP-CIAC-ML about 77.5%, and the proposed SO-APID-FT-DL-TDF-MFP significantly outperforms the others with approximately 96%. The proposed method demonstrates the highest F1-score performance, showcasing its superior capability in real-time transaction monitoring.

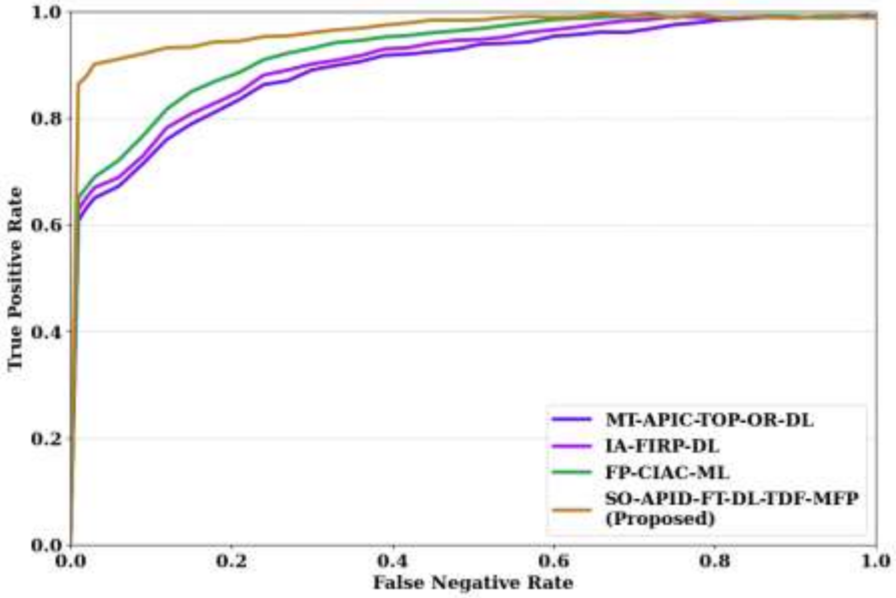


Figure 5. *Performance Analysis of Receiver Operating Characteristic (ROC)*

Figure 5 illustrates the performance analysis of the ROC curve for API-driven financial transactions in a deep learning-based threat detection framework. It evaluates the system's accuracy and efficiency in detecting threats within mutual fund processing, highlighting its effectiveness in distinguishing between legitimate and malicious activities. The ROC curve compares the true positive rate (TPR) against the false negative rate (FNR) for different models. The proposed method, SO-APID-FT-DL-TDF-MFP, starts at a TPR of approximately 0.62, quickly reaching 0.90 at a low FNR of around 0.02, and approaches 0.99. Existing methods, such as MT-APIC-TOP-OR-DL, IA-FIRP-DL, and FP-CIAC-ML, show lower TPRs, with the proposed method consistently outperforming them.

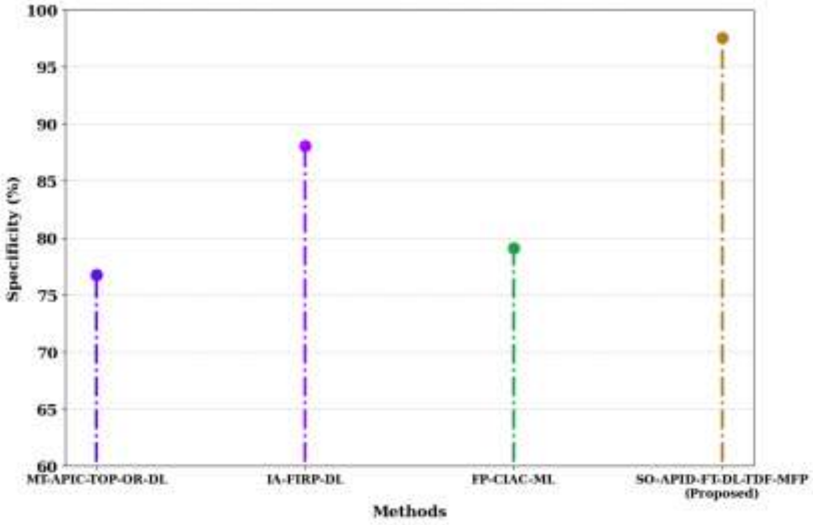


Figure 6. *Performance Analysis of Specificity*

Figure 6 illustrates the performance analysis of specificity in API-driven financial transactions, focusing on mutual fund processing. The graph compares the efficacy of a deep learning-based threat detection framework in identifying anomalies and fraudulent activities. It shows how the model's specificity improves over time, reducing false positives and ensuring accurate identification of legitimate transactions in a financial environment. MT-APIC-TOP-OR-DL achieves a specificity of approximately 76.7%, while IA-FIRP-DL shows a higher specificity of around 88.1%. FP-CIAC-ML reaches a specificity of about 79.1%. The proposed method, SO-APID-FT-DL-TDF-MFP, demonstrates the highest specificity at approximately 97.1%. Table 2 presents comparison results of the performance analysis.

Table 2. *Comparison results of the performance analysis*

Methods	Accuracy	Computational Time
Proposed SO-APID-FT-DL-TDF-MFP	97.5%	1.149
MT-APIC-TOP-OR-DL	95.5 %	1.290
IA-FIRP-DL	92.9 %	1.152
FP-CIAC-ML	85.8 %	1.353

Table 2 shows comparison results of the performance analysis. In the performance analysis, the accuracy of the methods is as follows: the Proposed SO-APID-FT-DL-TDF-MFP achieved the highest accuracy at 97.5%, followed by MT-APIC-TOP-OR-DL with 95.5%, IA-FIRP-DL at 92.9%, and FP-CIAC-ML with 85.8%. Regarding computational time, the Proposed SO-APID-FT-DL-TDF-MFP had the shortest time of 1.149 seconds, while MT-APIC-TOP-OR-DL took 1.290 seconds, IA-FIRP-DL required 1.152 seconds, and FP-CIAC-ML had the longest time of 1.353 seconds.

4. Conclusion

In conclusion, the SO-APID-FT-DL-TDF-MFP method presented in this paper demonstrates a secure optimization framework for API-driven financial transactions mutual fund processing. By integrating deep learning, this approach enhances security and efficiency, ensuring optimal performance and safeguarding data integrity. Its application in fintech enables better management of financial transactions, promoting trust and innovation within mutual fund processing systems. The proposed method is executed in Python. The proposed SO-APID-FT-DL-TDF-MFP achieves 98% precision, 97% recall, 96% F1-score, 97.1% specificity, 97.5% accuracy, and 1.149 seconds computational time, with a high ROC TPR of 0.99 at low FNR. The proposed framework for secure optimization of API-driven financial transactions using deep learning faces limitations such as the complexity of deep learning models, which may impact processing efficiency, and challenges in adapting to evolving attack patterns while ensuring privacy in sensitive transactions. Future work could focus on developing lightweight deep learning models for enhanced efficiency, implementing adaptive threat detection mechanisms to respond to new attack vectors, exploring federated learning for privacy-preserving techniques, and optimizing the scalability of the framework to handle large-scale financial systems.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Oladinni, A., & Adewale, G. T. *Innovative API frameworks and data-driven modelling for enhanced fintech lending applications.*

[2] Sreeravindra, B. B., & Gupta, A. (2024). Machine learning driven API data standardization. *International Journal of Global Innovations and Solutions (IJGIS*).

[3] Brown, E., & Johnson, M. (2022). API-driven fintech: Enhancing data access and security in financial services. *Advances in Computer Sciences, 5*(1).

[4] Singh, A. (2024). *API economy: Constraints to its growth and development* (Doctoral dissertation, University of Northern British Columbia).

[5] Reijnders, S., & Dhaenens, F. (2024). Enhancing financial transparency with API-driven tax reporting systems.

[6] Basheer, N., Islam, S., Alwaheidi, M. K., & Papastergiou, S. (2024). Adoption of deep-learning models for managing threat in API calls with transparency obligation practice for overall resilience. *Sensors, 24*(15), 4859. https://doi.org/10.3390/s24154859

[7] Yana, T., Dariya, K., Zinaida, B., & Adebayo, H. (2025). Advanced threat detection in API security: Leveraging machine learning algorithms.

[8] Isaac, L. D., Arunkumar, S., Sundaramurthi, V., & Bommannan, G. (2025, April). Revolutionizing financial analysis: A comprehensive framework for

predictive analytics, cryptocurrency trends, and text-based extraction in the financial data landscape. In *AIP Conference Proceedings* (Vol. 3279, No. 1). AIP Publishing.

[9] Adewale, T. (2025). *API-driven microservices for seamless integration across global supply networks.*

[10] Harris, H. (2025). *Transforming financial services through data sharing and innovation, remembering APIs, techniques.*

[11] Basheer, N., Islam, S., Alwaheidi, M. K., & Papastergiou, S. (2024). Adoption of deep-learning models for managing threat in API calls with transparency obligation practice for overall resilience. *Sensors, 24*(15), 4859. https://doi.org/10.3390/s24154859

[12] Sun, Y., & Li, J. (2022). Deep learning for intelligent assessment of financial investment risk prediction. *Computational Intelligence and Neuroscience, 2022*(1), 3062566. https://doi.org/10.1155/2022/3062566

[13] Lokanan, M. E., & Sharma, K. (2022). Fraud prediction using machine learning: The case of investment advisors in Canada. *Machine Learning with Applications, 8*, 100269. https://doi.org/10.1016/j.mlwa.2022.100269

[14] Bayya, A. K. (n.d.). *Cutting-edge practices for securing APIs in fintech: Implementing adaptive security models and zero trust architecture.*

[15] Brown, E., & Johnson, M. (2022). API-driven fintech: Enhancing data access and security in financial services. *Advances in Computer Sciences, 5*(1).

[16] University of New Brunswick. (n.d.). *CIC IDS 2017 Dataset.* https://www.unb.ca/cic/datasets/ids-2017.html

[17] Cheng, L., Zhang, J., Wang, Z., Liu, H., & Sun, Y. (2024). Implicit unscented particle filter based indoor fusion positioning algorithms for sensor networks. *Alexandria Engineering Journal, 94*, 104–119. https://doi.org/10.1016/j.aej.2023.09.001

[18] Castro-Correa, J. A., Gómez-Castaño, N., Ruiz-Lopera, J. A., & Escobar, D. A. (2024). Gegenbauer graph neural networks for time-varying signal reconstruction. *IEEE Transactions on Neural Networks and Learning Systems.* https://doi.org/10.1109/TNNLS.2024.3375839