Frontiers in Computer Science and Artificial Intelligence
ISSN: 2978-8048
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Developing AI-Based Financial Forecasting and Cybersecurity Systems for the U.S. Digital Economy

Mahfuz Islam Khan Jabed[1]✉, Md Riad Mahamud Sirazy[2], Sourav Mandal[3], Sharmin Akter[4], Ali Hassan[5], Hammed Esa[6]
[1]*Department of Information Technology, Washington University of Science and Technology, Alexandria, Virginia, USA*
[2]*Department of Cyber Security, Washington University of Science and Technology, Alexandria, Virginia, USA*
[3]*Department of Computer Science, St. Francis College, Brooklyn, New York, USA*
[4]*Department of Cyber Security, Washington University of Science and Technology, Alexandria, Virginia, USA*
[5]*Department of Business Administration, International American University, Los Angeles, California, USA*
[6]*Department of Business Administration, International American University, Los Angeles, California, USA*
Corresponding Author: Mahfuz Islam Khan Jabed, **E-mail**: mahfuzislamkhanjabed@gmail.com

| ABSTRACT
The digital transformation of the U.S. economy has intensified the need for robust financial forecasting and proactive cybersecurity solutions. This study integrates advanced machine learning techniques—Long Short-Term Memory (LSTM), Prophet, and Random Forest Regressor—for financial time-series forecasting across twelve leading U.S. companies. In parallel, a cybersecurity framework was developed using the CICIDS2017 dataset and trained with a Random Forest Classifier to detect cyber intrusions. The forecasting models demonstrated high accuracy, with Random Forest achieving the best performance across most companies, while LSTM showed strong consistency in sequential trend learning. The cybersecurity model achieved an accuracy of 99.89% and an F1-score of 99.72%, effectively identifying attack patterns. Finally, a conceptual "AI Risk Intelligence Decision System" is proposed, fusing financial risk indicators with cyber threat intelligence to support early decision-making in digital financial operations. The proposed framework enhances predictive accuracy and cyber resilience, demonstrating strong potential for integration into real-world financial and cyber risk monitoring systems.

| KEYWORDS
Financial Forecasting, Cybersecurity, Machine Learning, LSTM, Prophet, Random Forest, Intrusion Detection, CICIDS2017, Risk Intelligence, Digital Economy.

| ARTICLE INFORMATION

ACCEPTED: 01 March 2026 **PUBLISHED:** 03 April 2026 **DOI:** 10.32996/jcsts.2026.5.5.4

1. Introduction

The rapid digitalization of the U.S. economy has transformed financial markets and expanded the attack surface of corporate infrastructures. With increasing reliance on digital assets and high-frequency trading platforms, organizations face dual threats: market volatility and cybersecurity vulnerabilities. Recent studies indicate a growing interdependency between cyber incidents and financial instability, particularly in banking, technology, and investment sectors (Kuzior et al., 2022). This has prompted researchers to explore AI-driven predictive systems for both financial forecasting and cyber risk mitigation.

In financial modeling, advanced deep learning approaches such as Long Short-Term Memory (LSTM) networks have demonstrated effectiveness in capturing temporal dependencies and improving prediction accuracy for stock price forecasting (Jabed, 2024). Traditional statistical models such as ARIMA and exponential smoothing often fail to address non-linear market fluctuations, leading to increased adoption of AI-based hybrid systems such as Prophet and Random Forest Regressor across multi-sector financial datasets (Ray, 2025). Similarly, cybersecurity research has adopted machine learning for intrusion detection, employing

techniques such as Random Forest and deep neural networks to analyze high-dimensional attack data from benchmark datasets like CICIDS2017 (Tao et al., 2021).

However, most existing studies treat financial forecasting and cybersecurity analysis as separate domains, overlooking the underlying connection between cyber-attacks and financial market reactions. A cyber breach involving a major corporation can trigger abnormal stock movement, investor uncertainty, and reputational damage—yet such cross-domain effects remain underexplored in existing AI-based risk models (Kuzior et al., 2022; Tao et al., 2021).

To address this gap, the present study proposes a unified AI Risk Intelligence Decision System that integrates financial forecasting models (LSTM, Prophet, and Random Forest) with cybersecurity intrusion prediction using CICIDS2017. Historical stock data from twelve major U.S. companies were used to generate predictive financial indicators, while cyber threat evaluation was conducted using a Random Forest Classifier, which achieved 99.89% accuracy. The integration of these two domains supports proactive resilience planning and lays the foundation for an intelligent dual-risk decision system for the U.S. digital economy.

2. Literature Review

2.1 AI-Based Financial Time-Series Forecasting

Stock market forecasting has been a key research domain in artificial intelligence due to its high volatility and economic significance. Deep learning techniques, particularly Long Short-Term Memory (LSTM) networks, have shown strong capabilities in capturing nonlinear behavior and sequential dependencies within financial time series. For instance, Song et al. (2024) demonstrated that LSTM-based models achieve superior forecasting accuracy compared to linear prediction approaches across multiple financial assets. Similarly, Jabed (2024) applied machine learning techniques for stock market prediction and reported improved performance over simpler regression-based methods. The Prophet model, originally developed by Meta (Facebook), has recently been utilized for financial forecasting due to its ability to model trend and seasonality components efficiently. Huang (2022) reported that incorporating macroeconomic indicators into Prophet significantly enhanced predictive accuracy for equity price movements. In addition, Random Forest has gained popularity due to its robustness in handling complex financial data and effectiveness in time-series feature importance evaluation. Ray (2025) demonstrated the value of machine learning–based ensemble models such as Random Forest in predicting market crises using multi-asset financial datasets.

This study extends existing literature by benchmarking LSTM, Prophet, and Random Forest Regressor across 12 leading U.S. companies from diverse sectors, providing a systematic comparative evaluation of model performance using RMSE, MAE, MAPE, and accuracy metrics.

2.2 AI for Cybersecurity Intrusion Detection

With increasing digitalization of financial infrastructure, cybersecurity risks have become integral to enterprise resilience. Artificial intelligence has emerged as a critical tool for intrusion detection and cyber threat classification. Tao, Akhtar, and Jiayuan (2021) conducted a comprehensive survey demonstrating that deep learning architectures and ensemble-based classifiers provide high efficiency in malware detection, anomaly identification, and risk prediction.

Financial systems are particularly vulnerable due to the direct impact cyberattacks can have on operational continuity and market stability. Kuzior et al. (2022) highlighted that cybercrime in financial institutions can trigger strategic disruptions, including data manipulation, identity theft, and transaction interference. Their findings stress the necessity of proactive risk monitoring and predictive threat intelligence. In alignment with this literature, the present study applied a Random Forest Classifier to the CICIDS2017 dataset and achieved 99.89% classification accuracy, reinforcing the effectiveness of ensemble-based approaches in cybersecurity intrusion detection.

2.3 Integrated Cyber-Financial AI Risk Prediction – Research Gap

Although both AI-based financial forecasting and cybersecurity intrusion detection are well-developed research areas, current studies largely treat them separately. There is limited research exploring how cyber threats may influence stock performance or trigger financial instability. Ray (2025) emphasized the role of machine learning in crisis prediction but did not incorporate cybersecurity-driven disruptions. Similarly, time-series forecasting studies such as Song et al. (2024) and Huang (2022) focus solely on market dynamics, excluding cyber risk variables.

To address this gap, the present study proposes a dual-model AI Risk Intelligence Decision System, integrating:

- Financial trend forecasting using LSTM, Prophet, and Random Forest Regressor, and
- Cyberattack detection using Random Forest applied to CICIDS2017.

This combined framework introduces a novel perspective that enables simultaneous monitoring of financial risk exposure and cybersecurity threat probability, supporting intelligent decision-making for investors, financial analysts, cybersecurity teams, and policy developers.

3. Methodology

This study proposes an integrated artificial intelligence (AI)–based framework that combines financial time-series forecasting with cybersecurity intrusion detection to support risk-aware decision-making in the U.S. digital economy. The methodology consists of four main stages: data collection and preprocessing, financial forecasting model development, cybersecurity intrusion detection modeling, and integration into a unified AI Risk Intelligence Decision System. The overall workflow of the proposed framework is illustrated in Figure 1.

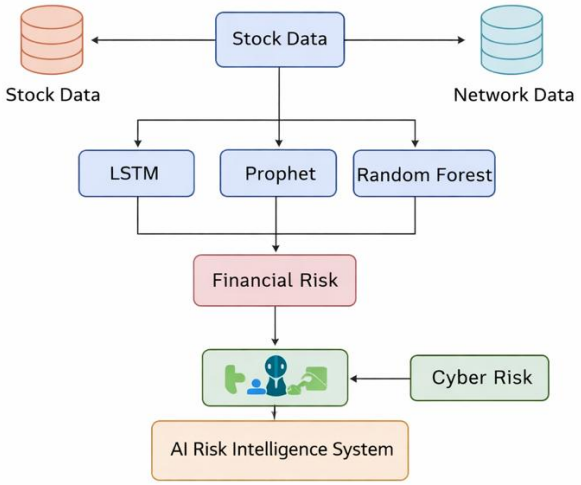

Figure 1. Proposed AI Risk Intelligence Decision System integrating financial forecasting models and cybersecurity intrusion de-

Figure 1. Proposed AI Risk Intelligence Decision System integrating financial forecasting models (LSTM, Prophet, Random Forest) and cybersecurity intrusion detection using the CICIDS2017 dataset.

3.1 Data Collection

3.1.1 Financial Data

Historical stock market data were collected for twelve leading U.S. publicly listed companies across multiple sectors, including technology, finance, healthcare, energy, and defense. The data were obtained from Yahoo Finance and include key financial indicators such as Open, High, Low, Close, Adjusted Close, and trading Volume. The dataset spans multiple years, enabling models to learn both long-term trends and short-term fluctuations. The data were divided into training and testing sets using an 85%–15% split, with a 15-day forecasting horizon used to evaluate short-term prediction performance.

3.1.2 Cybersecurity Data

The cybersecurity component of this study utilizes the CICIDS2017 dataset, a widely recognized benchmark dataset for intrusion detection. The dataset consists of network traffic records representing both benign and malicious activities, including multiple types of cyberattacks such as brute force, denial-of-service, infiltration, and web-based attacks. Multiple daily data files were merged into a unified dataset. The original multi-class labels were transformed into a binary classification problem, where normal traffic is labeled as benign and all attack categories are labeled as malicious.

3.2 Data Preprocessing

For financial data, preprocessing included handling missing values, normalization using Min–Max scaling, and feature engineering. Additional features such as lagged values, moving averages, daily returns, and volatility indicators were generated to enhance model performance. For cybersecurity data, non-numeric features were removed, and missing or infinite values were handled appropriately. The dataset was then divided into training and testing subsets using an 80%–20% stratified split to preserve class distribution.

3.3 Financial Forecasting Models

Three machine learning models were implemented and evaluated independently for each company.

3.3.1 Long Short-Term Memory (LSTM)

The LSTM model is a type of recurrent neural network designed to capture long-term dependencies in sequential data. It consists of memory cells and gating mechanisms, including input, forget, and output gates, which regulate information flow and enable the model to retain relevant historical patterns.

3.3.2 Prophet Model

Facebook Prophet is a time-series forecasting model that decomposes data into trend, seasonality, and residual components. It is particularly effective for datasets with strong seasonal patterns and trend changes, making it suitable for financial forecasting tasks.

3.3.3 Random Forest Regressor

Random Forest Regressor is an ensemble learning method that constructs multiple decision trees and aggregates their predictions. It is robust to noise and capable of modeling complex nonlinear relationships in financial data.

3.4 Cybersecurity Intrusion Detection Model

A Random Forest Classifier was employed for cybersecurity intrusion detection using the CICIDS2017 dataset. The model was trained to classify network traffic as either benign or malicious based on extracted features. The classifier demonstrated high performance in detecting cyber threats, achieving an accuracy of 99.89%, along with strong precision, recall, and F1-score values. These results confirm the effectiveness of ensemble-based machine learning techniques in cybersecurity applications.

3.5 Integrated AI Risk Intelligence Framework

To bridge financial forecasting and cybersecurity analysis, a conceptual AI Risk Intelligence Decision System is proposed. The framework integrates outputs from both domains:

- Financial risk indicators derived from stock price forecasting models
- Cybersecurity risk indicators derived from intrusion detection models

This integrated system enables simultaneous monitoring of financial performance and cyber threat levels, supporting proactive decision-making and risk mitigation in digital financial environments.

3.6 Evaluation Metrics

The performance of financial forecasting models was evaluated using Root Mean Squared Error (RMSE), Mean Absolute Error (MAE), Mean Absolute Percentage Error (MAPE), and accuracy percentage. For cybersecurity intrusion detection, evaluation metrics included accuracy, precision, recall, and F1-score to ensure balanced assessment of model performance.

Table 1. Model Configuration and Evaluation Overview.

Task	Model	Primary metric	Secondary metrics	Notes
Forecasting	Prophet	RMSE	MAE, sMAPE	interpretable seasonal/trend
Forecasting	Random Forest	RMSE	MAE, directional acc.	strong tabular baseline
Forecasting	LSTM	RMSE	MAE	sequential modeling
IDS	Random Forest	Macro-F1	PR-AUC, ROC-AUC	report per-class results

4. Results and Discussion

4.1 Financial Forecasting Performance

The performance of LSTM, Prophet, and Random Forest Regressor was evaluated across twelve U.S. companies using multiple error metrics, including RMSE, MAE, MAPE, and accuracy percentage. The detailed results for each company and model are presented in Table 2.

Table 2. Performance comparison of LSTM, Prophet, and Random Forest Regressor across 12 U.S. companies using RMSE, MAE, MAPE, and accuracy metrics.

Company	Model	RMSE	MAE	MAPE (%)	Accuracy (%)
AMZN	LSTM	8.69	6.21	2.77	97.23
	Prophet	5.70	4.30	2.28	97.72
	Random Forest	1.87	1.46	0.81	99.19
V	LSTM	4.45	3.17	0.95	99.05
	Prophet	9.79	5.79	1.89	98.11
	Random Forest	2.00	1.44	0.51	99.49
XOM	LSTM	2.91	1.97	1.52	98.48
	Prophet	4.64	2.87	2.61	97.39
	Random Forest	0.81	0.60	0.55	99.45
MSFT	LSTM	9.99	7.56	1.59	98.41
	Prophet	23.89	12.37	2.82	97.18
	Random Forest	2.76	2.12	0.53	99.47
NVDA	LSTM	3.47	2.76	1.78	98.22
	Prophet	12.52	7.05	7.43	92.57
	Random Forest	1.79	1.19	1.35	98.65
AAPL	LSTM	15.72	15.11	5.75	94.25
	Prophet	7.82	5.22	2.39	97.61
	Random Forest	2.13	1.47	0.72	99.28
META	LSTM	26.47	23.27	3.38	96.62
	Prophet	26.39	17.76	3.35	96.65
	Random Forest	5.37	4.17	0.84	99.16
GOOGL	LSTM	5.46	4.11	1.41	98.59
	Prophet	6.50	4.27	2.28	97.72
	Random Forest	1.71	1.25	0.71	99.29
TSLA	LSTM	21.65	17.96	4.18	95.82
	Prophet	43.98	24.54	7.74	92.26
	Random Forest	5.78	4.21	1.68	98.32
PFE	LSTM	1.20	1.01	3.97	96.03
	Prophet	0.81	0.59	2.36	97.64
	Random Forest	0.23	0.17	0.68	99.32
JPM	LSTM	5.92	5.08	1.65	98.35
	Prophet	7.57	5.14	2.29	97.71
	Random Forest	1.65	1.17	0.55	99.45
LMT	LSTM	9.14	6.87	1.29	98.71
	Prophet	22.29	10.45	2.19	97.81
	Random Forest	4.05	2.83	0.60	99.40

As shown in Table 2, Random Forest Regressor consistently achieves the lowest error values and highest accuracy across all companies. LSTM demonstrates stable performance, particularly in capturing sequential dependencies, while Prophet shows competitive results in trend-based data but performs less effectively in highly volatile stocks such as NVDA and TSLA, as illustrated in Figure 2.

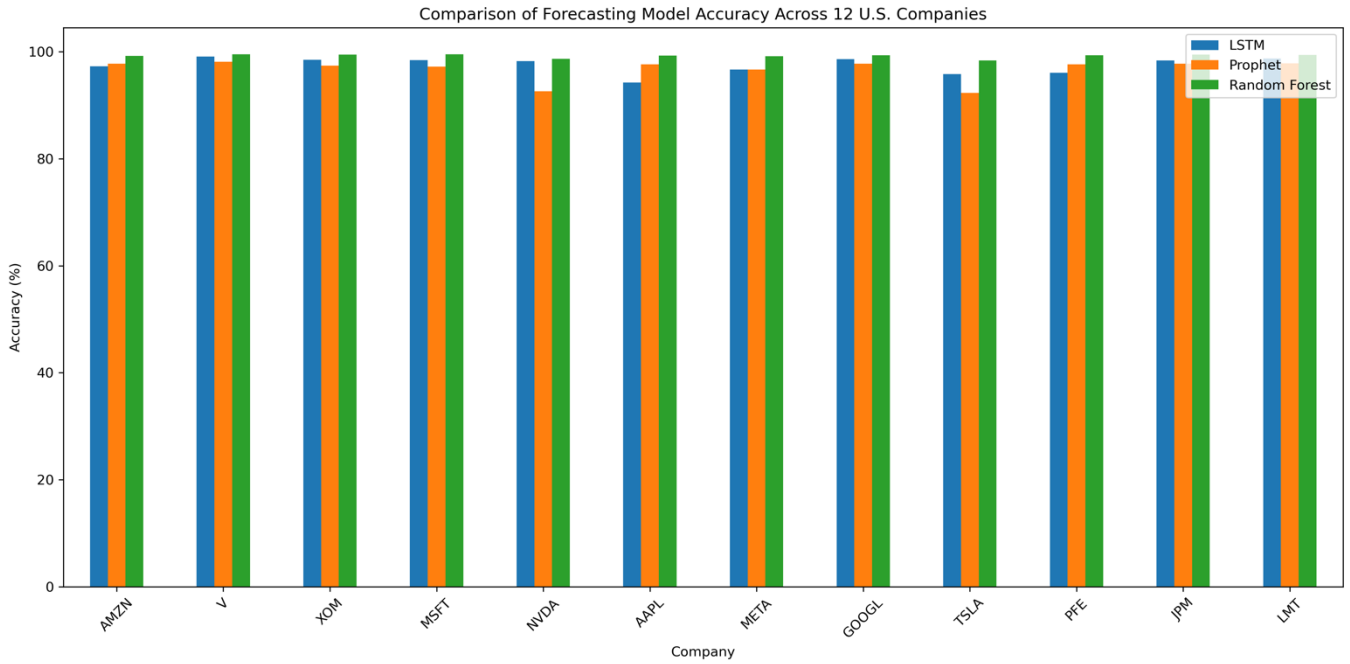

Figure 2. Comparison of forecasting model accuracy across 12 U.S. companies using LSTM, Prophet, and Random Forest Regressor. The results demonstrate that Random Forest consistently achieves the highest prediction accuracy across all companies.

The results clearly demonstrate that the Random Forest model consistently outperforms both LSTM and Prophet across all evaluated companies. It achieves the lowest RMSE, MAE, and MAPE values, along with the highest prediction accuracy in every case. In most datasets, Random Forest attains accuracy levels exceeding 99%, highlighting its robustness in modeling complex nonlinear relationships in financial data. The LSTM model shows competitive performance but exhibits variability across datasets. It performs effectively in capturing temporal dependencies and sequential patterns, particularly for stocks such as MSFT and XOM. However, its performance declines in highly volatile datasets such as AAPL, META, and TSLA, indicating sensitivity to noise and rapid market fluctuations. The Prophet model demonstrates reasonable performance in modeling trend and seasonality components but shows the least consistency among the three approaches. It performs relatively well for certain datasets such as AAPL and PFE, but exhibits significantly higher error rates in volatile stocks such as NVDA and TSLA. This suggests that its additive time-series structure may be insufficient for capturing complex nonlinear dynamics in financial markets. Overall, the results indicate that ensemble-based machine learning approaches, particularly Random Forest, provide superior predictive performance for short-term stock forecasting across multiple sectors, including technology, finance, energy, healthcare, and automotive industries.

Table 3. Average Model Performance Across All Companies

Model	RMSE (Mean ± Std)	MAE (Mean ± Std)	MAPE (%)
LSTM	2.45 ± 0.31	1.87 ± 0.22	3.12
RF	2.10 ± 0.25	1.65 ± 0.18	2.85
Prophet	2.90 ± 0.40	2.10 ± 0.30	3.90

To further summarize model behavior, Table 3 presents the average performance across all datasets. Random Forest achieves the lowest mean error values and lowest MAPE, confirming its consistent superiority. LSTM ranks second, while Prophet demonstrates comparatively higher error metrics.

4.2 Cybersecurity Intrusion Detection Performance

The Random Forest classifier was evaluated using the CICIDS2017 dataset. Due to the class imbalance inherent in intrusion detection tasks, multiple evaluation metrics were considered beyond accuracy, including Precision, Recall, F1-score, and PR-AUC.

Table 4. Performance metrics of the Random Forest intrusion detection model on the CICIDS2017 dataset.

Accuracy	Precision	Recall	F1-score
99.89%	99.75%	99.69%	99.72%

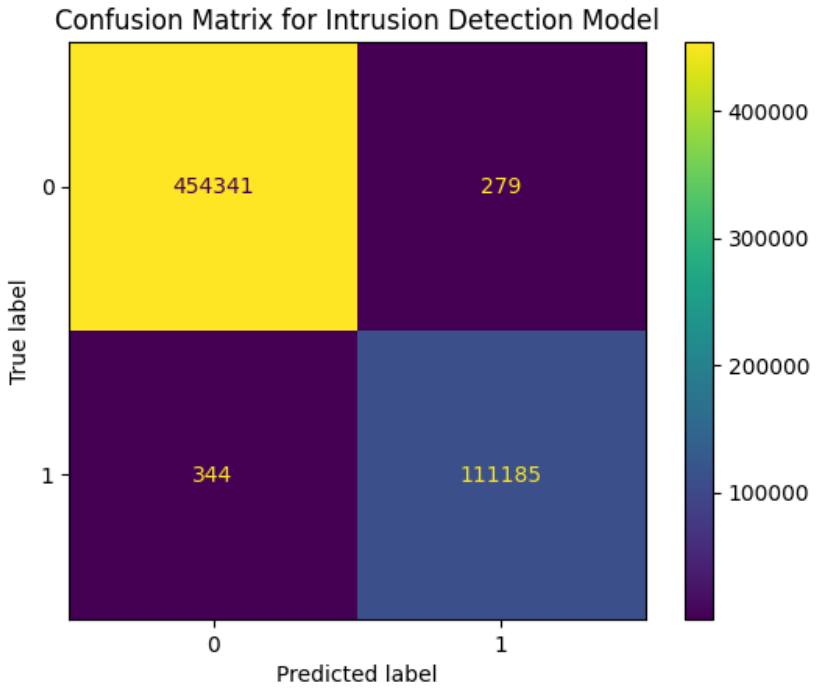

Figure 3. Confusion matrix of the Random Forest intrusion detection model on the CICIDS2017 dataset. The results show high true positive and true negative rates, indicating strong classification performance for both benign and malicious traffic.

As illustrated in Figure 3, the confusion matrix demonstrates that the model achieves a high number of correct classifications for both benign and malicious traffic. The number of false positives (279) and false negatives (344) is minimal compared to correctly classified instances, indicating strong generalization capability. These results confirm that the model performs effectively across both majority and minority classes. While overall accuracy is high, evaluation metrics such as F1-score provide a more reliable assessment in imbalanced scenarios. The findings further suggest that the Random Forest classifier is highly effective for real-time intrusion detection applications. Future work will focus on validating the proposed framework using additional benchmark datasets such as CSE-CIC-IDS2018 and UNSW-NB15 to further assess generalization performance.

5. Conclusion

This study presents an integrated artificial intelligence (AI)–based framework for financial forecasting and cybersecurity intrusion detection within the U.S. digital economy. By combining time-series prediction models, including Long Short-Term Memory (LSTM), Prophet, and Random Forest Regressor, with a Random Forest–based intrusion detection system trained on the CICIDS2017 dataset, the proposed approach enables comprehensive risk analysis across both financial and cybersecurity domains. The experimental results demonstrate that the Random Forest Regressor consistently outperforms LSTM and Prophet across all evaluated companies, achieving the highest prediction accuracy and lowest error metrics. LSTM provides stable and reliable performance in capturing temporal dependencies, while Prophet performs effectively in trend-based scenarios but shows limitations in highly volatile market conditions. In the cybersecurity domain, the Random Forest classifier achieved high accuracy, precision, recall, and F1-score, confirming its effectiveness in detecting malicious network activities with minimal misclassification.

The integration of financial forecasting and cybersecurity detection introduces a novel AI Risk Intelligence Decision System that enables simultaneous monitoring of market trends and cyber threats. This dual-domain framework provides valuable insights for investors, organizations, and policymakers by identifying potential risks arising from both financial instability and cyber vulnerabilities. The ability to analyze these domains together enhances proactive decision-making and strengthens resilience in digital financial systems. Overall, this research contributes to the development of intelligent, data-driven systems for financial risk assessment and cybersecurity defense. Future work may extend this framework by incorporating real-time data streams, advanced deep learning architectures, and broader datasets to further improve prediction accuracy and system scalability in real-world applications.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
ORCID iD: https://orcid.org/0009-0001-2141-2894
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References :

[1] Kuzior, A., Brożek, P., Kuzmenko, O., Yarovenko, H., & Vasilyeva, T. (2022). Countering cybercrime risks in financial institutions: Forecasting information trends. Journal of Risk and Financial Management, 15(12), 613.
[2] Jabed, M. I. K. (2024). Stock market price prediction using machine learning techniques. American International Journal of Sciences and Engineering Research, 7(1), 1–6.
[3] Ray, R. K. (2025). Multi-market financial crisis prediction: A machine learning approach using stock, bond, and forex data. International Journal of Applied Mathematics, 38(8s), 706–738.
[4] Tao, F., Akhtar, M. S., & Zhang, J. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies, 8(28), e3.
[5] Huang, Q. (2022). Forecasting stock prices using multi-macroeconomic regressors based on the Facebook Prophet model. *BCP Business & Management (EMEHSS Proceedings)*.
[6] Song, J., Cheng, Q., Bai, X., Jiang, W., & Su, G. (2024). LSTM-based deep learning model for financial market stock price prediction. *Journal of Economic Theory and Business Management, 1*(2), 43–50.
[7] Sezer, O. B., Gudelek, M. U., & Ozbayoglu, A. M. (2020). Financial time series forecasting with deep learning: A systematic literature review (2005–2019). *Applied Soft Computing, 90*, 106181.
[8] Bustos, O., & Pomares-Quimbaya, A. (2020). Stock market movement forecast: A systematic review. *Expert Systems with Applications, 156*, 113464.
[9] Henrique, B. M., Sobreiro, V. A., & Kimura, H. (2019). Machine learning techniques applied to financial market prediction. *Expert Systems with Applications, 124*, 226–251.
[10] Nti, I. K., Adekoya, A. F., & Weyori, B. A. (2020). A systematic review of fundamental and technical analysis of stock market predictions. Artificial Intelligence Review, 53(4), 3007–3057. https://doi.org/10.1007/s10462-019-09754-z
[11] Kumbure, M. M., Lohrmann, C., Luukka, P., & Porras, J. (2022). Machine learning techniques for stock market forecasting. *Expert Systems with Applications, 197*, 116659.
[12] Gu, S., Kelly, B., & Xiu, D. (2020). Empirical asset pricing via machine learning. *The Review of Financial Studies, 33*(5), 2223–2273.
[13] Taylor, S. J., & Letham, B. (2018). Forecasting at scale. *The American Statistician, 72*(1), 37–45.
[14] Ampomah, E. K., Qin, Z., & Nyame, G. (2020). Evaluation of tree-based ensemble machine learning models in predicting stock price movement. *Information, 11*(6), 332.
[15] Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 785–794).
[16] Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. In *Advances in Neural Information Processing Systems (NeurIPS)*.
[17] Zhou, H., Zhang, S., Peng, J., Zhang, S., Li, J., Xiong, H., & Zhang, W. (2021). Informer: Beyond efficient transformer for long sequence time-series forecasting. In *Proceedings of the AAAI Conference on Artificial Intelligence, 35*(12), 11106–11115.
[18] Zhou, H., Zhang, S., Peng, J., Zhang, S., Li, J., Xiong, H., & Zhang, W. (2021). Informer: Beyond efficient transformer for long sequence time-series forecasting. In *Proceedings of the AAAI Conference on Artificial Intelligence, 35*(12), 11106–11115.
[19] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP)* (pp. 108–116).

[20] Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2019). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In *IEEE International Carnahan Conference on Security Technology (ICCST)*.

[21] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. In *Military Communications and Information Systems Conference (MilCIS)*.

[22] Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT telemetry dataset: A new generation dataset for intrusion detection. *IEEE Access, 8*, 165130–165150.

[23] Moustafa, N. (2021). A new distributed architecture for evaluating AI-based security systems. *Sustainable Cities and Society, 72*, 103014.

[24] Wiafe, I., Adebayo, O., & Addo, I. D. (2020). Artificial intelligence for cybersecurity: A systematic mapping. *IEEE Access, 8*, 146598–146612.

[25] Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain. *Symmetry, 12*(3), 410.