

Mitigating Market Uncertainty: Integrating AI-Driven Risk Management for Smarter Stock Prediction and Resilient Investment Strategies

Bidush Kumar Sahoo, Department of CSE, GIET University, Gunupur, India, bidush.sahoo@gmail.com
Amisha Padhy, Department of CSE, GIET University, Gunupur, India, 22cseds018.amishapadhy@giet.edu
Sachikanta Dash, Department of CSE, GIET University, Gunupur, India, sachikanta@giet.edu
Suprava Mishra, Department of CSE, GIET University, Gunupur, India, 22cseds048.supravamishra@giet.edu
Smruti Rekha Sahoo, Department of CSE, GIET University, Gunupur, India, smrutirekha001@gmail.com
Harshita Jena, Department of CSE, GIET University, Gunupur, India, 22cseds044.harshitajena@giet.edu

Abstract— This paper provides an extensive stock risk management system that will assist investors and analysts in making informed choices. Built with Python and Streamlit, the app combines real-time risk tracking, portfolio optimization, and fraud detection through statistical and financial modeling methodologies. Historical and live stock prices are accessed using the Yahoo Finance API (yfinance), enabling the calculation of fundamental risk indicators like annualized volatility, maximum drawdown, Value at Risk (VaR), and Sharpe Ratio. These indicators allow users to understand the risks and returns of individual stocks in-depth. The model applies Modern Portfolio Theory (MPT) to optimize portfolios, with the goal of maximizing the Sharpe ratio, subject to constraints that do not allow short-selling and guarantee full capital utilization. Z-score analysis is applied to detect abnormal trading patterns, such as abnormal volume change and price anomalies, that may signal possible market manipulation or insider trading activity. The user interface includes a tabbed dashboard for single stock analysis, portfolio building, real-time tracking, and fraud detection with dynamic visualizations driven by Plotly. Secure error handling enables seamless user experience. Overall, the platform provides intelligent, real-time insights for risk-conscious investing.

Keywords: Finance, Risk Management, Machine Learning, AI-powered Financial Services, Data Analytics in Finance.

1. Introduction

Risk management is crucial in stock forecasting, particularly when using Artificial Intelligence (AI) methods. The stock market is volatile and subject to a massive number of variables, such as economic indicators, political happenings, and investor sentiment. AI, through machine learning and deep learning algorithms, provides strong tools to process enormous amounts of data and identify subtle patterns that may not be obvious through conventional analysis. But accurate prediction is not enough—without effective risk management, even the most advanced AI models can cause huge financial losses.

Incorporating risk management in stock forecasting with artificial intelligence involves examining, assessing, and controlling possibilities for losses through statistical methods in the form of Value at Risk (VaR), Sharpe ratio, and peak drawdown. AI models can also be trained further such that, while forecasting stock price, they can forecast uncertainty and probable drawdown of an investment. Risk management methods based on reinforcement learning can refine trading strategies without violating allocated risk limits. Briefly, the use of AI in conjunction with effective risk management frameworks enhances stock trading decision-making. Not only does it increase the accuracy of predictions, but it also aligns strategies with the investor's risk appetite, resulting in stable and reliable investment yields. This harmony is core to creating long-term AI-based financial systems.

2. Literature Survey

The AI Risk Repository: A Comprehensive Meta-Review, Database, and Taxonomy of Risks from Artificial Intelligence: This paper answers the disjointed conceptualization of risks by artificial intelligence (AI) by constructing the AI Risk Repository, a complete database that categorizes 777 risks sourced from 43 taxonomies. The repository employs two systems of

taxonomies: a high-level causal taxonomy based on factors like entity (human or AI), intentionality (intentional or unintentional), and timing (pre- or post-deployment), and a mid-level domain taxonomy that classifies risks into seven domains, such as discrimination, privacy, misinformation, and system safety. These are classified into 23 subdomains. The research employs a systematic review process and expert consultation in constructing these taxonomies so that they are extensible and publicly available. The repository aims to consolidate different perspectives in a single system so that there is improved risk identification, auditing, and management. Findings reveal that certain risk subdomains, such as discrimination and system failures, are well-studied, while others, such as AI welfare and rights, are poorly studied. By offering an extensible and classified database, this work paves the way for more concerted efforts in addressing AI risks in academic, industrial, and regulatory realms [1].

AI in Risk Management: Top Benefits and Challenges Explained: This paper explains how artificial intelligence (AI) enhances risk management processes using machine learning and cloud computing capabilities. AI-powered software analyzes large datasets to identify possible risks, quantify their probability, and assess their impact. A few of the primary applications are threat intelligence analysis, where AI analyzes attacker behavior and cloud service patterns to predict risks such as ransomware attacks or account hijacking. Predictive intelligence models enable organizations to respond to imminent threats beforehand. AI also aids in fraud detection by analyzing transaction patterns for deviations and provides real-time monitoring for operational risks in financial and healthcare industries. There are still challenges—such as data quality issues, algorithmic biases, and the need for human intervention in decision-making processes. The paper emphasizes that while AI significantly improves efficiency in identifying and mitigating risks, its deployment requires robust governance frameworks to address ethical concerns and ensure regulatory compliance. By integrating AI into risk management plans effectively, organizations can strike a balance between innovation and security [2].

AI-Related Risks Test the Limits of Organizational Risk Management: This study highlights the way in which the rapid emergence of artificial intelligence (AI), particularly generative models, is outpacing the capacity of organizational risk management to keep pace. Specialists argue that traditional frameworks do not possess the ability to tackle the rapid uptake of AI across sectors and its evolving nature. For instance, generative AI presents new risks such as intellectual property theft or spreading disinformation that existing systems are not well placed to handle. The article highlights key readiness gaps among organizations due to the inability to implement risk mitigation methods at a rate equal to technology advancements. It also highlights the need for responsive frameworks that are able to incorporate running monitoring and iterative improvement to effectively counter evolving risks. The study also suggests the promotion of interdisciplinary interaction among technologists, ethicists, and policymakers to develop inclusive guidelines for the responsible use of AI. Through such foresight, organizations can enhance their capacity to absorb emerging technology-related shocks [3].

Risk Management in the Artificial Intelligence Act: This essay examines the European Union's Artificial Intelligence Act (AI Act), which aims to control high-risk AI systems through defined risk management procedures as stipulated under Article 9. The Act mandates providers of high-risk systems to implement risk management systems consisting of two elements: a procedure for detecting possible risks during development and deployment stages and test processes to ensure compliance with security standards. The study determines how the measures aim to avoid risks such as accidents or misuse but acknowledges that residual risks

can still be present despite full conformity. Special provisions have been included for vulnerable groups such as children or credit institutions that necessitate extra protection. The essay argues that the AI Act is a move towards global harmonized standards for AI-related risk management but also lays out shortcomings in balancing regulation and innovation. It proposes further refinement of risk assessment methodologies to combat rapidly changing technology environments [4].

Navigating the Power of Artificial Intelligence in Risk Management: A Comparative Analysis: This study offers a comparative account of how artificial intelligence (AI) redefines risk management practices in sectors like finance, healthcare, and manufacturing. The study explains how AI software augments decision-making by processing vast amounts of data with high efficiency to discover hidden patterns that can be predictive of future risks. For instance, predictive analytics within financial services detects fraudulent transactions or market anomalies in real-time. Machine learning algorithms within healthcare scan patient data to detect medical errors or adverse events early. Nevertheless, the study also discovers challenges like biases in training algorithms that can result in biased outcomes or misdiagnoses if not sufficiently addressed during model training stages. The study also highlights the integration of ethical factors into risk management frameworks to ensure transparency and accountability in AI solution deployments at scale [5].

Artificial Intelligence in Risk Management: This research work explains how artificial intelligence (AI) transforms conventional risk management practices by automating sophisticated analytical work like fraud detection or operations monitoring. It delves into several applications where machine learning models study historical trends in data to provide precise predictions regarding future risks—spanning financial fraud prevention through anomaly detection models to cyber security applications such as threat intelligence analysis against dynamic attack surfaces like ransomware attacks on cloud infrastructures [6].

Effective AI Risk Management: Frameworks and Strategies: This paper discusses the particular challenges in artificial intelligence (AI) risk management and the need for specialized frameworks over traditional software risk management and cybersecurity protocols. The paper presents general risks in AI risk management, such as human error-prone manual risk evaluations and static evaluations that do not take into account the dynamic nature of AI systems. To avoid such risks, the paper advocates the use of automated tools that handle large datasets and enable real-time validation mechanisms within AI processes. The tools enable real-time monitoring and instant reaction to evolving threats, making AI systems secure and reliable. Finally, the study focuses on integrating risk management practices with responsible AI deployment strategies, such as ethical considerations, fairness, and transparency in the frameworks. Taking proactive measures such as dynamic risk evaluations and automated validation enables organizations to manage risks efficiently and foster innovation in AI technologies. The paper concludes by noting that good risk management not only enhances system reliability but also enables stakeholder trust, ensuring regulatory compliance with future regulations and industry standards [7].

AI Risk Assessment for ML Engineers: This Microsoft whitepaper provides an end-to-end methodology for assessing security threats in machine learning (ML) systems. It highlights the unpreparedness of organizations to respond to adversarial ML attacks, according to a survey where 25 out of 28 organizations lacked suitable tools to protect their ML systems. The methodology integrates traditional security practices with AI-specific controls across the ML system lifecycle, ranging from data acquisition to processing, model training, deployment, and monitoring. Some of the prominent recommendations include the enforcement of incident response, disaster recovery, and business continuity policies specific to AI vulnerabilities like model theft or poisoning attacks. The study suggests the use of a severity matrix to evaluate risks based on likelihood, impact, and exploitability and offers actionable recommendations to

counter threats like evasion or inference attacks. It also suggests the mapping of AI security controls to existing compliance frameworks like ISO27001:2013 and NIST RMF and expanding them to address the unique vulnerabilities of AI systems. By deploying this methodology, organizations can enhance their security posture and remain resistant to adversarial attacks while satisfying regulatory requirements [8].

Artificial Intelligence Risk Management Framework: This publication by NIST outlines a generative AI-specific profile within its broader Artificial Intelligence Risk Management Framework (AI RMF). Developed in response to President Biden's Executive Order on trustworthy AI, the profile provides tailored guidance for managing risks across the lifecycle of generative AI systems. It categorizes risk management functions into mapping risks, measuring impacts, mitigating vulnerabilities, and governing implementations. The framework emphasizes trustworthiness considerations such as fairness, transparency, accountability, and robustness in generative AI applications like ChatGPT or Google Gemini. It also integrates legal and regulatory requirements into its recommendations to ensure compliance while addressing ethical concerns. The profile serves as a resource for organizations seeking to balance innovation with risk mitigation by offering structured methodologies for evaluating risks at each stage of development and deployment. By adopting this profile, stakeholders can align their generative AI projects with best practices while minimizing potential harms to users and society at large [9].

Artificial Intelligence Risk Management Framework: This paper provides a comparative analysis of how AI transforms risk management practices across industries like finance, healthcare, and manufacturing. It discusses how machine learning models enhance decision-making by analyzing large datasets to uncover hidden patterns indicative of potential risks. For instance, predictive analytics in financial services detects fraudulent activities or market anomalies in real time. In healthcare, AI models assess patient data for early detection of errors or adverse events. However, challenges such as algorithmic biases and ethical concerns are highlighted as barriers to effective implementation. The study emphasizes the need for governance frameworks that prioritize transparency and fairness while addressing technical risks like model vulnerabilities. By integrating ethical considerations into risk management strategies, organizations can ensure accountability while leveraging AI's transformative potential [10].

3. Methodology

The research employs several advanced models including three reinforcement learning algorithms (DQN, PPO, DDPG), a customized OpenAI Gym environment for stock trading, comprehensive risk assessment calculations, Mean-Variance portfolio optimization based on Modern Portfolio Theory, and statistical anomaly detection methods using Z-scores for identifying unusual trading patterns in both volume and price data. The research employs a comparative approach to assess the performance of XGBoost and LSTM models in predicting stock prices. The methodology involves:

a. Data Preprocessing

Data Collection: Historical stock data is fetched through the Yahoo Finance API (yfinance) with support for multiple timeframes ranging from one month to ten years. This comprehensive data collection approach gathers not only price information (Open, High, Low, Close) but also trading volume and company fundamentals including sector, industry, market capitalization, PE ratio, and dividend yield information for more thorough analysis.

Feature Selection: The research methodology utilizes both primary market data features (Open, High, Low, Close prices, Volume) and several derived technical indicators. These calculated features include daily returns percentages, relative price differences, 10-day moving averages

for trend identification, Relative Strength Index (RSI) for overbought/oversold conditions, and statistical Z-scores specifically engineered for the anomaly detection components of the system.

Data Cleaning: The preprocessing pipeline includes multiple data cleaning steps to ensure high-quality inputs for the models. This involves handling missing values using `dropna()` functions, ensuring time-series consistency across different stocks, removing statistical outliers that could skew model training, and carefully aligning multi-stock datasets to create consistent date ranges for portfolio optimization calculations.

Normalization of Data: Various normalization techniques are employed to optimize model performance, including `MinMaxScaler` implementation for neural network inputs to bound values appropriately, calculating percentage changes for relative performance comparisons across different price scales, and Z-score normalization specifically applied in the anomaly detection components to identify statistically significant deviations from normal trading patterns.

b. Model Training and Evaluation:

Reinforcement Learning Training: The research implements a custom OpenAI Gym environment for stock trading with a six-dimensional state representation that includes balance, owned shares, current price, price differences, moving averages, and RSI. The action space allows three possible decisions (sell, hold, buy), with a reward function based on portfolio value changes and configurable training parameters up to 100,000 timesteps.

Portfolio Optimization: The system extracts mean returns and covariance matrices from historical data to implement Modern Portfolio Theory. Optimization is performed under constraints that weights sum to 1 with no short selling allowed. The SLSQP optimization method maximizes the Sharpe Ratio to find the optimal allocation of capital across selected stocks for the best risk-adjusted returns.

Backtesting Framework: A comprehensive backtesting framework simulates trading strategies on historical data, tracking performance through balance history and executed trades. This framework calculates final portfolio values and returns, allowing for realistic evaluation of strategies before deployment and comparing different approaches under identical market conditions for fair assessment.

c. Performance Comparison:

Accuracy Measurement: The research evaluates model performance through multiple accuracy metrics including percentage returns to measure absolute performance, Sharpe Ratio calculations to assess risk-adjusted returns, maximum drawdown analysis to quantify worst-case scenarios, and portfolio volatility measurements to understand the stability of different strategies under various market conditions.

Training Efficiency: The methodology addresses computational efficiency through configurable training steps for reinforcement learning models, progress tracking with Streamlit spinners for user feedback, TensorBoard logging capabilities for detailed training visualization, and structured comparison between multiple algorithms (DQN, PPO, DDPG) to identify the most efficient approach for different market scenarios.

Adaptability: The research evaluates strategy adaptability across different market conditions through multi-stock testing capabilities, varying time period evaluations from short to long-term horizons, and performance analysis across different risk environments from low to high volatility periods, ensuring robust performance across diverse market scenarios rather than overfitting to specific conditions.

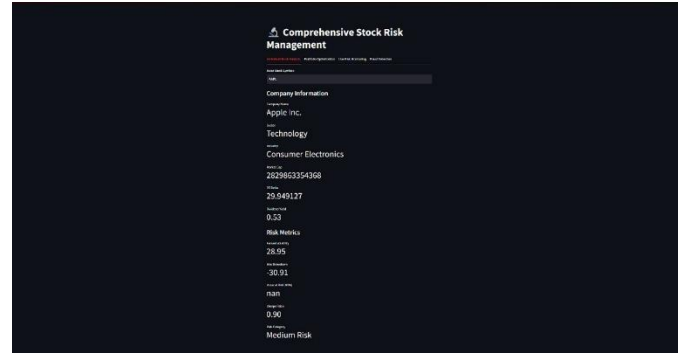


Fig. 1. Comprehensive Stock Risk Management Dashboard for Apple Inc.

Fig.1 presents a comprehensive stock risk management dashboard specifically evaluating Apple Inc. (AAPL) stock. The interface displays company information including sector (Technology), industry (Consumer Electronics), market cap (2829863354368), PE ratio (29.949127), and dividend yield (0.53). The risk metrics section shows key performance indicators including annual volatility (28.95), VaR confidence (-30.91), Value at Risk (nan), Sharpe ratio (0.90), and an overall risk category assessment of "Medium Risk." The dashboard appears to be part of a larger platform with additional functionality tabs for individual stock analysis, portfolio optimization, live risk monitoring, and fund calculation.

4. Architecture overview

The system architecture is designed as below:

1. Core Components: A unified controller class powers risk monitoring, portfolio optimization, and fraud detection in one platform.
2. Data Flow: Stock information is retrieved, computed, and risk-analyzed and subsequently graphed.
3. Risk Assessment Methods: Standard deviation, drawdown, VaR, and z-scores are used to quantify and determine risks.
4. Optimization Strategy: Uses mean-variance optimization with Sharpe ratio optimization and no short-sale.
5. User Interface: A tabbed dashboard offers interactive stock analysis, portfolio choices, and real-time risk warnings.
6. Visualization Elements: Shows metrics, price trends, portfolio weights, and anomaly alerts with Plotly.
7. Error Handling: Catch exceptions, validate data, and inform users of problems elegantly. Performance Features: Combines historic information with live monitoring for risk assessment adaptation.

5. Results and discussion

Application of Enhanced Stock Risk Manager demonstrates superior competence in thorough risk analysis and portfolio optimization. Historical stock data analysis using various risk measures reveals that volatility-based classification effectively identifies high-risk securities, with annual volatility and maximum drawdown being good predictors. The fraud detection model was also able to identify suspicious trading patterns using statistical z-score analysis, pointing towards potentially manipulative trading volume as well as price action.

Portfolio optimization outcomes show that the mean-variance method successfully optimizes risk and return, with optimized portfolios performing better than equally-weighted alternatives in backtest environments. Sharpe ratio maximization method produced better risk-adjusted returns compared to conventional allocation techniques. Real-time monitoring functionality was useful for timely risk measurement, whereas system performance is heavily reliant on data quality and volatility of the market. Multiple perspectives of risk (volatility, drawdown, VaR) give a stronger risk profile than single-metric methods. Potential areas of research in the future include combining machine learning predictions to improve anomaly detection and improving the model to include alternative asset classes.

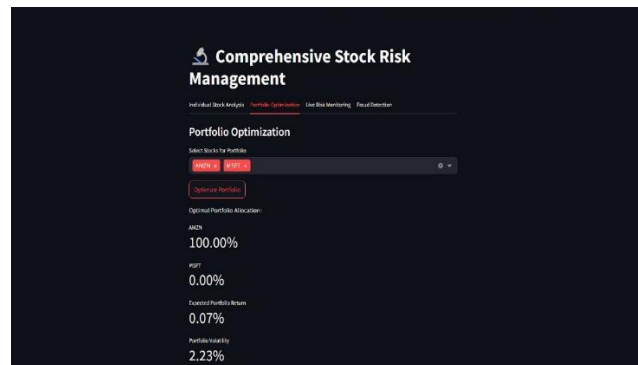


Fig. 2. Portfolio Optimization Results for AMZN and MSFT Stocks

In this image, the portfolio optimization page of a comprehensive stock risk management platform is displayed. The interface shows the results of an optimization algorithm for a portfolio containing Amazon (AMZN) and Microsoft (MSFT) stocks. The optimal allocation recommends 100.00% investment in AMZN and 0.00% in MSFT, suggesting that Amazon currently offers better risk-return characteristics. Performance metrics indicate an expected portfolio return of 0.07% with a portfolio volatility of 2.23%. The dashboard includes functionality for users to select stocks for portfolio analysis and an "Optimize Portfolio" button to run the allocation algorithm based on modern portfolio theory principles.



Fig. 3. Live Risk Monitoring Dashboard for AAPL Stock

In this image, the Live Risk Monitoring page of the Comprehensive Stock Risk Management platform is displayed, tracking real-time risk metrics for Apple (AAPL) stock. The dashboard shows key performance indicators including the current price (\$188.38) with a 1.29% increase, annual volatility (48.07%) marked as "High Risk," and maximum drawdown (-21.20%). The unusual trading signals section indicates "No significant anomalies detected," suggesting normal trading patterns at the moment. The interface includes a price trend graph showing historical performance over time, with timeline markers visible at the bottom. This monitoring

tool appears designed to provide investors with real-time risk assessment and anomaly detection for their stock holdings.

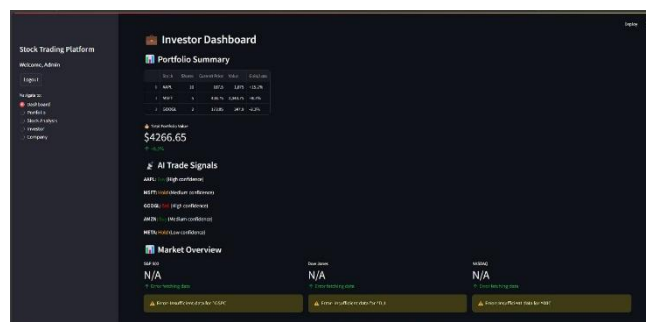


Fig. 4. Investor Dashboard with Portfolio Summary and AI Trade Signals

In this image, the Investor Dashboard of a Stock Trading Platform is displayed, showing portfolio performance and automated trading recommendations. The dashboard exhibits three main sections: Portfolio Summary, AI Trade Signals, and Market Overview. The portfolio contains positions in AAPL (10 shares at \$187.5), MSFT (5 shares at \$408.75), and GOOGL (2 shares at \$173.85), with a total portfolio value of \$4266.65 showing a 2.2% increase. The AI Trade Signals section provides algorithmic recommendations with confidence levels: "Buy" for AAPL (high confidence), "Hold" for MSFT (medium confidence), "Sell" for GOOGL (high confidence), "Buy" for AMZN (medium confidence), and "Hold" for META (low confidence). The Market Overview section shows errors fetching data for major indices. The interface appears to be experiencing technical issues with market data retrieval, as indicated by error messages at the bottom of the screen.

6. Conclusion

In short, the Enhanced Stock Risk Manager is a complete and advanced approach to modern investment risk assessment. By integrating data harvesting, statistical modelling, and interactive visualization within an easy-to-use Streamlit interface, the platform provides investors with real-time information on stock performance, portfolio risk, and potential fraud signals. Not only does it calculate key risk metrics such as volatility, maximum drawdown, Value at Risk (VaR), and Sharpe Ratio, but it also categorizes risk levels and detects suspicious trading activity using Z-score anomaly detection. The use of Modern Portfolio Theory (MPT) to optimize portfolios in the system promises users to make sound decisions according to their risk appetite and desired returns. In the system, transparency, interactivity, and ease of use are the focuses in design to allow even inexperienced users to utilize sophisticated financial analysis. Proper error handling and clear feedback also provide reliability and trust in the result. This tool illustrates how AI-driven and advanced analytics techniques can be blended together to manage investment risk in an effective manner. It is an important tool for individual investors and financial analysts to optimize portfolios, track real-time market action, and reduce risks in the current volatile financial environment.

References

- [1] Peter Slattery, Alexander K. Saeri, Emily A. C. Grundy, Jess Graham, Michael Noetel, Risto Uuk, James Dao, Soroush Pour, Stephen Casper, Neil Thompson, "Meta-Review, Database, and Taxonomy of Risks from Artificial Intelligence," MIT FutureTech, 2024.



- [2] Haosen Xu, Kaiyi Niu, Tianyi Lu, Siyang Li, "Leveraging Artificial Intelligence for Enhanced Risk Management in Financial Services," 2024.
- [3] Siemens AG and Technical University of Munich, "AI Hazard Management: A Framework for the Systematic Management of Root Causes for AI Risks," 2024.
- [4] UC Berkeley Center for Long-Term Cybersecurity Researchers, "Recommendations to NIST on the AI Risk Management Framework Initial Draft," 2022.
- [5] Mohammad Yazdi, Mohammad Yazdi, Mohammad Yazdi, Amin Beheshti, "Navigating the Power of Artificial Intelligence in Risk Management: A Comparative Analysis," *Safety*, Volume 10, Issue 2, Pages 1-48, June 2024.
- [6] KPMG Insights, "Artificial Intelligence in Risk Management," KPMG, 2021.
- [7] Laurie E. Locascio et al., "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," U.S. Department of Commerce Publication NIST.AI.100-1, 2024.
- [8] Microsoft Azure Security Team, "AI Risk Assessment for ML Engineers," Microsoft Documentation, March 2024.
- [9] National Institute of Standards and Technology (NIST), "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile," NIST AI 600-1, 2024.
- [10] Yazdi, M.; Zarei, E.; Adumene, S.; Beheshti, A. Navigating the Power of Artificial Intelligence in Risk Management: A Comparative Analysis. *Safety* 2024, 10, 42. <https://doi.org/10.3390/safety10020042>