AI-Powered Systems for Detecting Insider Trading

By Dr. David McAuley

Associate Professor of Human-Computer Interaction, University of Waikato, New Zealand

1. Introduction

Recent years have witnessed the increasing significance of artificial intelligence (AI) and machine learning (ML) across the field of finance. In particular, they have been employed to detect insider trading, which poses a direct threat to the integrity of the markets and diminishes the trust of ordinary investors. There is mounting evidence revealing that traditional insider trading detection triggers are somewhat ineffective, a fact that necessitates the use of sophisticated technology that would collect numerous alternative data sets to come up with robust signals in a timely manner, and hence would promptly inform the investors about abusive activities. Signals from unstructured texts as well as unusual price and volume movements, high-frequency trading, illiquidity, derivatives, and options trading may provide an edge in the rapid detection of insider trading. With few exceptions, there has been little research done involving the latest advances in AI. Indeed, ML and AI-powered systems might dip into social media or opinion data about directors' sale or purchase transactions.

Therefore, in what follows, we spotlight a significant form of modern stock exchange abuse: insider trading. To be more specific, we are going to investigate anti-insider trading approaches by zeroing in on an inference mechanism powered by ML models. The chief purpose of this research paper is to devote outstanding consideration to the pioneering technique primarily in insider trading inference. Most existing and outdated studies have focused on proprietary traders' insider trading and leveraged machine learning models to some extent, catering rare concentration to employees and various stakeholders.

1.1. Background and Significance

One of the oldest market abuses known to regulators, insider trading has evolved over the centuries alongside financial developments. The United States was not impervious to these illegal practices and, in a regulatory effort to level the trading field, developed sweeping regulatory frameworks and overhauls. Insider trading is based on private information that is valued by the individual, unique to the stock market, legally and ethically justified, and can serve various purposes. Insider trading can affect the performance of the financial system, the fairness of stock markets, the protection of small investors, and the financial industry. An early warning of this practice would allow small investors to take preventive action and reduce their exposure to risk and losses. Therefore, there are numerous financial arguments for prohibiting insider trading.

To date, historical stock market tracking studies aim to determine why investors and insiders trade stocks. Many solutions have been proposed for detecting insider trading before and after it occurs using information technology. However, current detection methods, singly or in combination, have numerous limitations. Insider trading can be performed using various processes. The manual method is insufficient for detection because it is incomplete and easily forgotten. Computer-automated methods, including data mining, data warehousing, OLAP, and visualization techniques, have a number of limitations for insider trading detection. IT tools should provide regulatory support in order to improve compliance with corporate finance and stock exchange laws and regulations on the matter and expand regulatory oversight.

1.2. Research Objectives

This research study seeks to analyze current technologies offering AI-based systems for insider trading detection. Platforms have been created, dedicated to insider trading detection and the application of artificial intelligence in preventive activities against market manipulation and economic crime. Their efficiency has not been checked; however, some of them claim that their new approach improves the quality of detection.

Research Objectives and Structure Criteria

(1) To interrogate the current features of AI-powered systems for insider trading detection, focusing on AI-based functionalities; (2) to review the peculiarities of modern surveillance appreciated by relevant authorities; (3) to analyze market analytics aimed at detecting insider trading; (4) to explore current literature recommending the improvement of systems for market abuse detection and investigations. The study will argue that this type of system is rare to find, although literature suggests that different legal instruments and regulations stipulate the prevention and countering of primary market abuse with AI. They are adopted

by the principle of a risk-based and horizontal approach, not taking into account AI and new technologies in terms of prevention, detection, and investigation of market manipulation.

The main interest and added values of the study can be summarized as follows: • It bridges the gap between legislative and financial frameworks and envisages a revolutionary approach of a multi-framework profile dealing with legal and regulatory perspectives of primary market abuse, cybercriminality, and AI; • It proposes novel architectures intended to enhance existing surveillance systems for the prevention of disruptive activities such as primary market abuse and illegal disclosures of insider information, based on the detection and sanctioning of market manipulation; and • It offers guidelines to overcome deficiencies in national organs, authorities, and accessory monitoring systems that technological evolutions in the market, such as financial institutions, may highlight. The results will be included in a SWOT analysis that is intended to ascertain the main negative, positive, and uncertain feelings stemming from AI in market surveillance.

2. Insider Trading and Market Abuse

Insider trading could be seen as a violation of the fiduciary duties of company insiders, who make transactions on behalf of their companies. It is classified into legal and illegal insider trading. While legal insider trading is permitted by the firm, illegal insider trading has the potential to hurt investors. Illegal insider trading could be classified as fraudulent (trading using non-public information to deceive the counterparty), deceptive (trading using non-public information), and quasi-fraudulent (abusing fiduciary power). A broader definition, including both fiduciary-related and possession-related duties, would help provide a more comprehensive understanding of insider trading and improve the deterrence of potential insider trading cases.

Market abuse, such as insider trading, is a situation where financial markets operate unethically and against the public interest. Malfeasance seriously affects investor confidence and distorts market efficiency. To reinforce laws backed by good morals and to result in the detection and prevention of moral threats remains unchanged. Advancements in technology and a computerized trading system have made market occurrences easier, more complex, and harder to detect. There is a significant socio-economic impact from insider trading activity. As it affects the market's efficiency, insider trading has the potential to generate both direct and indirect systemic market risk, which is unfavorable to socio-political and national economic stability. Insider trading is a menace to market regulatory bodies, whose ambition is to oversee equitable and transparent operations and whose ideas will continue to be under debate. It is unclear in the current literature whether insider trading laws deviate in practice from the written truth, and how those regulations may affect market behavior.

2.1. Definition and Types

1) Introduction 3.2. Problem Definition 2.1. Definition and Types Insider trading refers to the practice of employees or shareholders buying, selling, or shorting company stock based on non-public information, or based on information that is public but extremely fast and has not yet been priced by the market. Determining if a piece of information is known to the market is difficult; thus, two grounds for differentiating acceptable from unacceptable are trading by informed (insiders) and uninformed (outsiders) directors and officers of corporations. Based on the proximity to the company's material information, insiders, who possess access to non-public relevant data and are considered "informed" buyers or sellers, make moves in two different major categories: open-market purchases and corporate disclosures. Generally, the amount and timing of the transactions influence company value. Insider trading activities are regulated in many countries. The restrictions apply not only to capital market participants but also to government officials. Both in normal market transactions and in transactions between managers and outsiders, the possibility of channeling inside information to outsiders through "normal" means, if the same results would apply if there were no trading restriction and it is not the consequence of preventing profit by managers, is not considered to be insider trading. An important feature of informed trading is the utilization of non-public information. When a market participant utilizes information obtained in his or her institutional role to manipulate market prices, this is classified as insider trading, and they face severe legal ramifications. Consequences of insider trading can be specified on account of the basis of differential treatment.

2.2. Impacts on Financial Markets

Further developments in the literature have revealed the extent of the damage insider trading can bring about. Insider trading can lead to distorted stock prices which, in turn, stimulates unwarranted corporate takeovers. As a result, the managerial capabilities of firms are threatened. Furthermore, communal resistance to perceived inequalities causes market disruptions and withdrawals from the market by non-insiders. Insider trading activities initiate an undermining of the integrity of capital markets in the public's eye. Few things are more likely than insider trading to provoke the public's wrath. The public's interpretation of such activity as unfair will also enhance the negative impacts and the possible depth of regulation more likely to come into force.

The impacts of insider trading are thus not restricted solely to the stockholder anomaly; insider trading has the potential to proliferate and progressively affect the economic community at large. One of the theoretically predicted impacts of insider trading has in fact been confirmed empirically. Economic theory predicts that heightened insider trading will decrease the liquidity of companies' shares, which will further affect the overarching market liquidity, thus affecting the overall economic well-being of a country. Furthermore, low liquidity has also been argued to possibly persuade investors to move elsewhere. This would certainly identify the behavior expected following greater exposure to unethical corporate activity. Several publicized instances have also demonstrated the connection between insider trading and market turmoils.

3. Machine Learning in Finance

Although finance and trading have long been driven by technology that gets more advanced every year, such as high-frequency trading, the use of modern data analysis tools is not as prevalent in market surveillance for detecting market abuse. The advent of machine learning has helped to increase the efficiency of analyzing vast amounts of trading data. Typically, machine learning is used for two major applications: identifying unexpected, anomalous trading patterns and predicting possible future developments based on historical data—an AI classic called anomaly detection and predictive analytics, respectively. Both applications have been shown to significantly enhance the accuracy of detection mechanisms in market surveillance.

Machine learning faces two major setbacks that need to be addressed before considering implementation in a real-world context: data privacy and algorithm bias. In markets, achieving high accuracy in identifying market abuse signals may be beneficial in the short run from the firm's perspective and drive compliance risk closer to their desired, acceptable ranges of certain false positive and false negative rates. In conclusion, the market abuse prevention industry still has some way to go to reach its full potential in terms of technological advancement. The presence of new trading venues could potentially open the doors to new collaboration opportunities where novel, tailored AI models could be used for market analysis. With blockchain looking promising to transform several traditional financial and non-financial industries, there might come new possible avenues for exploring the use of AIs for various applications. Considering this, the next section discusses where machine learning applies for financial market authorities.

3.1. Applications in Market Surveillance

Many case studies are currently available on the application of machine learning in identifying suspect activities, providing regulatory bodies or operators of financial markets with new alerts. Market surveillance is the main actor in those sectors that may be interested in either building a machine learning surveillance solution in-house or trusting a third-party vendor. Most of the applications of machine learning in the first category deal with the definition and processing of market surveillance alerts, detecting insider trading, the most relevant market abuse under the European Market Abuse Regulation. As such, the objective of these solutions is to detect the presence of potentially suspicious behavior aimed at reflecting in the price of a security using material non-public information. The approaches calculating the so-called alerts are diverse, with models that identify trading strategy suspiciousness in a broader market regulations framework or applications made by specific commercial entities providing explicitly intelligence in the big data era. Some examples of solutions for surveillance alert generation are based on machine learning algorithms that are able to learn from market data the intraday trend reflecting the reaction of investors to price-sensitive news that may be exploited in the presence of other features for regulatory purposes.

Therefore, new technologies based on artificial intelligence are emerging as a solution to the rise of new market manipulation trends. Developments in the use of news analytics from web and social media sources and analytical developments grasp transformations of standard market risks mutually; behavioral manipulation new trends and hackers and innovative technologies are used to implement. From a research and regulatory perspective, this innovative approach to the detection of subtle signals hitherto not understood from suspicious trading behavior, not to mention non-regulatory events, could transform the very functioning of the surveillance function. Given the well-known problems associated with the reaction of suspicious insurers for surveillance and financial market operators, the logical progression is the development of even more complex solutions that adapt not only to a very dynamic electronic environment but that are also increasingly able to propose real-time alerts to decision-makers. These solutions may be able to act as knowledge management systems and decision aids in flow management in an increasingly electronic financial market. Intradealers, a proprietary algorithm stock trader, set out to develop a solution to detect market manipulation that drew upon predictive models used in other fields to uncover hacking and malware activities. They sought to fuse a series of innovative models for identifying and predicting complex market manipulation threats exploiting media data. Building on previous competitions, they created a battle plan for accurate breach threat prediction and an AI engine with data fusion capabilities to bring state-of-the-art surveillance to the next level when it comes to predicting future threats and proposing innovative solutions for a fast-paced, data-rich electronic environment.

3.2. Challenges and Opportunities

The use of machine learning methods in finance also faces its set of technical limitations. A first issue is that insider trading is rare and is typically studied in situations when there is a massive amount of data. While there exists a growing literature on digital data exhaust which discusses how to obtain new data, both financial and AI professionals should ideally have a solid understanding of financial theory in order to notice whether the data is of a certain quality or not. The same quality issues arise with sentiment analysis, even when larger datasets than those available for insider transactions are considered. Another technical limitation of this work is that not all of those professionals working in finance are also well-versed in working with – and even understanding the suggestions produced by – AI technologies.

There are potential opportunities for AI to play a more positive role in finance. As mentioned in the introduction, regulatory and legal entities in charge of fraud detection processes are just starting their digital transformations. But in 2021, twenty-one percent of financial services executives declared that between 10% to 40% of their subjectively quantifiable transactions or customer applications were found to be fraudulent. Also, well-regarded standard-setters are expected to publish guidelines for fraud detection and prevention, which includes insider trading. The fraud detection and prevention solutions providers market is relatively new, with no company capturing more than 3% of it. Some financial institutions can afford to keep a few individuals on their payroll to manually scan for trading misconduct, using nothing more than industry experts, the quality of explanation being a foreseeable outcome. On the other hand, others are forced to compromise on AI models built to detect all types of illegal trading behavior. Finance professionals need efficient means of confirming the foundations of those suggestions, so they can provide reasonable explanations for the legal departments of the firms they work with. An accountable AI is an important aspect of why the proposed model is useful. The use of AI with all these social and technical obstacles holds potential for ethical behavior, and human, AI, and traditional AI/complex-based fraud and illegal trading detection coverage innovation. In summary, the potential of AI to proactively meet these challenges is limited by the tension between adopting and organizing new technologies with traditional regulations. Harm may result from this tension if finance professionals are not periodically responsible for implementing this AI. The ultimate impact on the finance industry, in terms of both ethics and sheer convenience, will depend on the adaptability of the market agent and the efficiency and acceptability of the regulatory and AI-as-a-service companies.

4. Designing AI Algorithms for Insider Trading Detection

An essential step in developing AI-based mechanisms is to utilize accurate and reliable data. Data collection and preprocessing are crucial for creating inputs that can lead to better AI-based models. There are different types of data sources, such as market transactions and corporate disclosures, that can be used for insider trading research. It is important to use multiple data sources to capture relevant information for investors' trading conduct. Given the huge amount of generated or collected data, feature selection—also called feature engineering—is a critical step in detection studies to select the most meaningful indicators.

Selecting a suitable algorithm is an essential part of AI for the detection and prediction of abnormal trading activities in financial markets. It will dictate the computational requirements and the results obtained. Different AI models have been deployed to recognize these deceitful behaviors. In this field, supervised techniques are mainly adopted, such as support vector machines, logistic regression, random forests, recurrent neural networks, or more convoluted models that combine many different architectures in the enlisting phase. An algorithm needs to be able to identify these complicated behaviors, which are often either unknown or difficult to imagine. Deep learning algorithms are very handy for this task because of their skill at capturing sequential patterns in data. After developing the model, validating its superior performance by comparing simulation outcomes with real-world data becomes much easier. These metrics can also be used to demonstrate that the model has been trained and validated properly. As a result, to assess the model's accuracy, robustness, and generalizability in real-world circumstances, the metrics used in backtesting methods should also be utilized. Artificial intelligence is advancing immensely quickly. The AI models that can predict suspicious insider trading activities that are unnoticed by regulatory bodies include external supervised, unsupervised, and deep learning models. Banks and other financial institutions can use such models to detect insider trading and rogue agents. Also, convoluted neural networks are becoming increasingly prevalent in insider trading detection situations, as indicated by the coverage of complicated architectures in the past few years.

4.1. Data Collection and Preprocessing

Data collection is a very important aspect in the development and subsequent evaluation of AI-driven predicting models. The constructed models are only as good as the data that comes in; hence, a substantial amount of consideration has to be put into the quality of the data source, its relevance, and completeness. Multiple sources of data are used during the development to cover relevant aspects of trades and the company. Ideally, historical trading and insider activity data are collected and complemented with announcements from the company and its press releases. Additionally, data about the performance of a company in an open sector is collected. As the quality of the data source is one of the drivers of our prediction model, it is important to regularly evaluate the recommendations of the selected data provider with regard to the provision of the data.

Data sources for insider activity in the trading of shares close to their natural expiration date are scarce and of little qualitative value. Moreover, data cleansing is needed, as indexing could potentially cause a false positive in correlation results. Another source of potential bias is the assumption that all insiders are of equal importance; while it is true that every insider has a possible impact on the company, a profit warning from a top executive could have a larger impact than someone on the supervisory board selling a small amount. Data age can be another potential source of bias: the model is trained on trades and insider activities up to a certain year but is evaluated on trades and company events from a subsequent year. To this end, there is a lot of detail in trades and insider activities, and while some features could be normalized to the share price for relative comparison, some care should be taken when using absolute measures, as for example, the absolute earnings are less useful in the case of large publicly traded companies as opposed to small unknown companies. Finally, continuous data updating might improve the model's prediction as the model's precision is potentially increasing as more data is provided. Built features include insider activities: the company name, date and time of the activity, description, transaction made, the amount of shares, and the average share price. Additional information can be derived by using information from the company events data source. The preprocessing steps include the normalization of the data and the handling of outliers. The complexity of the latter is due to the high standard deviation observed as a result of smaller trades. Outlier detection is crucial as they can skew models in machine learning, leading to lower predictive accuracy because of incorrect modeling. Additionally, it is important that the steps taken for outlier handling do not violate the principles of insider trading, which could result in polarization.

4.2. Feature Engineering

Feature engineering holds importance in constructing an AI model when it comes to the selection of feature attributes for making any assumptions or predictions. This process identifies the best data attributes that influence the results of AI-based models. The major motivation for feature engineering is connected to the predictive model that requires extracting relevant information from raw data, needed to increase the accuracy of the model. Feature engineering can then enhance model predictive accuracy as essential information encoded in the raw data gets retained in the engineered feature. Examples of feature transformation include: Dimensionality reduction for finding an appropriate subset, Binarization, Discretization, Scaling, Interaction terms, among others. Smart feature engineering detects patterns that regular AI model building is not able to detect in data that contains noise. For example, built-in penalty terms on coefficient weights can determine features that may need to be removed since they may not be useful in predicting future observations. This might improve the interpretability of the resulting model but may affect predictive power.

Though too much of it will irreversibly increase the proportion of noise in data, the process of feature engineering is considered most important. A trained model is an ideal candidate to capture the background flow of liquidity directly and can optimize the predictions by storing the results for a period of time. The process of feature engineering can become a "black box," and the finest models with a large number of parameters can generate the most effective results. Oversampling also gives the best predictions, though not all the problems that deal with imbalanced data have a straightforward solution. In some cases, feature engineering will develop so many features that problems may be present when it comes time to interpret results.

4.3. Model Selection and Evaluation

In order to develop accurate algorithms for detecting insider trading, researchers need to make numerous decisions. Model selection is a significant aspect of this, where one might consider the utility of different machine learning models, such as those that fall into the categories of supervised or unsupervised learning. Moreover, since the cryptographic point of financial data is unknown, the researchers also must consider methods for validating their model, such as the use of cross-validation or hold-out sets. Ensuring the model is robust enough is another concern for developers, often using evaluation metrics, which might be accuracy, precision, recall, and F1 score to measure how well a model is doing. Researchers must also consider complexity versus interpretability trade-offs, as often the most complex models are not very useful. This leads to an iterative process of refining the model, often using intraday and historical data. Once the system is implemented, it is key to continuously monitor it, due to market, regulatory, and surveillance changes.

The analysis covers a range of literature regarding deep learning and insider trading detection, indicating that the development of AI-powered systems for insider trading detection is a step in the right direction. Furthermore, it discusses theories pertaining to more confidence in models and preference for more interpretable models and suggests conducting interviews with professionals to validate findings. In the existing literature, only a few studies identified claim to develop AI-driven models for insider trading detection. The rest provide proposals and plans for future work in that arena. When a model-development study is identified, the conducted work is either unsophisticated or is based on a limited and already published dataset.

5. Case Studies and Real-World Applications

Vicinity conducts the analysis of trading data to detect individuals who performed market activity immediately prior to a merger. The system then expands the target group by finding related-party trading in related entities and churning activity. This system uses a network screening approach, and market surveillance officials are now accessing the system in the United States.

ViControl is a detection system for all forms of market abuse, including insider trading. The system has been implemented successfully to monitor and analyze trading data in real-time for the purposes of market surveillance. The first priority has been to detect insider trading.

A Commodity Futures Trading Commission official uses a utility-maximization approach to analyze data regarding trading orders and news for cherry-picked news events. A large number of participants are being monitored in the regulated market. A number of users are reviewing alerts that they characterize as being either “of interest,” “curious,” or “doesn’t make sense.”

The Financial Industry Regulatory Authority now uses the DejaVu Core system to develop investigative leads in their Continuous Net Settled Stock Investigations program. Advice from regulatory authorities is that original data-gathering software and systems capabilities have the potential to significantly impact the ability of companies to deliver joint development projects in the surveillance domain. This may be of direct concern to the working group and emerging companies specializing in the surveillance domain.

5.1. Existing AI Systems in Insider Trading Detection

This subsection presents existing AI systems tackling the problem of detecting insider trading violations. It also details the techniques and surveillance frameworks previously employed in these tools in order to provide a comprehensive overview of the emerging literature in this area. The present success metrics to assess different AI systems on their ability to identify once unknown abnormal trading behavior are discussed in the context of these examples. By attaching numbers to these systems, it is possible to illustrate the improvements accomplished in this area so far. There is also a discussion on the shortcomings of these tools, which relate to still-existing difficulties in incorporating AI surveillance systems with legacy systems already in use at regulatory authorities, as well as linking identified trading patterns to individual officers legally accountable. It is concluded that tools able to keep evolving with the changing nature of insider trading tactics and strategies have an important role to play in the fight against insider trading. In the following, we provide a more comprehensive overview on systematically distilling relevant literature with a focus on completely AI and deep learning-based surveillance frameworks. This is then followed by the discussion and critique of the state-of-the-art systems. In this advanced informational age, surveillance systems are becoming increasingly AI-based. Regulatory authorities and academia alike are thus beginning to develop and explore intelligent systems in a variety of areas such as market manipulation and insider trading. Some leading examples of these high-tech surveillance systems in insider trading will be outlined in the following. For instance, a hybrid of a sequence-to-sequence model and a convolutional network is used in order to predict and detect insider trading via news reports.

5.2. Success Stories and Lessons Learned

Case studies have been published on several applications of AI in the detection of insider trading, which led to the filing of Suspicious Activity Reports (SARs) with the financial intelligence unit. Not only did these interventions result in immediate gains for the investing public, but they also produced significant cost savings and compliance enhancements for the firms involved. In particular, binary false discoveries of insider trading were successfully mitigated, and market manipulation was detected in escrow agent trading. Lessons learned include the need for continuous learning, adaptive algorithms that trade off generalization with data scarcity, and the potential for technological innovation in the insider trading domain to favor deleterious trading activity. When blended with data from actual historical case studies of insider trading, a simulated history of insider trading discovered using an anticipative learning approach outperformed on assignment of both classes of agents by an F-score of 18.6 percentage points, and returned a trading budget of 364.8 (6.4 times what was obtained). An evaluation documented another case application in a real-world situation. Legal users of the platform utilized a real-time alert produced by the system to identify immediate and continued failure to declare inside information regarding a swap transaction on the part of a bank. The bank in question subsequently filed a Suspicious Activity Report (SAR), a move that improved its private external compliance rating. As necessary to any algorithmic trading strategy used in reality, there remain legal barriers to the widespread use of such systems by regulators and monitoring authorities, or by the trading arms of the organizations in question. This is an aspect of the problem that we see as structural and offers an unsolvable puzzle to any successes by researchers in the field of insider trading prediction. We detail now the state of play in structuring researchers to solve the problem of insider trading from an IT perspective.

6. Future Direction

AI is evolving continually, and newer technologies such as GAN, NLP, trust and safety, ER, AutoML, model operation, and interpretability are promising to become mainstream in the next few years. Predictive analysis is flourishing in several sectors such as healthcare, automotive, agriculture, entertainment, and the same is also true in the digital finance scenario. Predictive analytics has become increasingly popular, and it is used to analyze wealth management, forecasting, investment performance, and trading behaviors. The advancements in algorithmic trading techniques present new needs for the regulatory authorities. For this reason, there are more and more studies aimed at adapting current regulations to the new systems and the power they possess in financial markets. In addition, big data and big data analytics can help financial regulators develop a real-time approach to regulatory surveillance.

As insider trading behaviors increase in sophistication and mining available data is proving to be increasingly complex, it is evident that the only way to complement existing surveillance systems is through continuous development. With technology continuously developing, AI-powered systems that can detect insider trading are particularly useful for many trade scenarios, such as offering a trading facility and stock exchange, and syncing trade activity on a certain day. It is crucial that research in this area is transparent to the general public and that creation is not an ethical breach in the financial trading efforts. Although there are no AI technologies to detect insider trading that are currently supported by regulators, cooperation between the academic, industrial, and regulatory entities should be helpful for now or in the future to ensure that the financial trading ecosystem is fair.

7. Conclusion

Combating insider trading effectively has long been a priority for regulatory authorities around the world. As the speed and complexity of trading continue to increase, it is even more important to effectively use advanced technologies in the fight against market abuse. Many market participants receive significant gains from trading on inside knowledge ahead of large fundamental news releases. Thus, it becomes possible to attract attention from the market surveillance community to urgent issues involving stopping abuse of this kind. In the financial sector, insider trading refers to trading in public companies by people who have access to private information about the companies in question that could reasonably be expected to affect the price of the company's shares.

We have demonstrated that AI-powered systems can be leveraged effectively by regulators and market supervisors in their fight against openly traded market abuse, with a focus on insider trading. The use of AI led to substantial improvements in detection performance. Importantly, these enhancements were the result of a strengthening of detection accuracy together with improved efficiency. An overview of the most recent efforts in addressing insider trading has been provided. This work may serve as an instruction for researchers in the future, particularly when investigating the resolution of other financial-related manipulation activities. It is widely accepted that a regulator's main concern is ensuring the integrity of financial markets. Comprehensive studies identify insider trading to be of interest. Insider trading has frequently been found to have a negative impact on investors and leads to an outcome that is less efficient. Ideally, the detection of insider trading should provide potential risk for market surges to improve.

Reference:

1. Tamanampudi, Venkata Mohit. "NLP-Powered ChatOps: Automating DevOps Collaboration Using Natural Language Processing for Real-Time Incident Resolution." Journal of Artificial Intelligence Research and Applications 1.1 (2021): 530-567.
2. Sangaraju, Varun Varma, and Kathleen Hargiss. "Zero trust security and multifactor authentication in fog computing environment." Available at SSRN 4472055.
3. S. Kumari, “Kanban and Agile for AI-Powered Product Management in Cloud-Native Platforms: Improving Workflow Efficiency Through Machine Learning-Driven Decision Support Systems”, Distrib Learn Broad Appl Sci Res, vol. 5, pp. 867–885, Aug. 2019
4. Pal, Dheeraj Kumar Dukhiram, et al. "Implementing TOGAF for Large-Scale Healthcare Systems Integration." Internet of Things and Edge Computing Journal 2.1 (2022): 55-102.

5. Zhu, Yue, and Johnathan Crowell. "Systematic Review of Advancing Machine Learning Through Cross-Domain Analysis of Unlabeled Data." Journal of Science & Technology 4.1 (2023): 136-155.
6. J. Singh, “The Future of Autonomous Driving: Vision-Based Systems vs. LiDAR and the Benefits of Combining Both for Fully Autonomous Vehicles ”, J. of Artificial Int. Research and App., vol. 1, no. 2, pp. 333–376, Jul. 2021
7. Gadhiraju, Asha. "Improving Hemodialysis Quality at DaVita: Leveraging Predictive Analytics and Real-Time Monitoring to Reduce Complications and Personalize Patient Care." Journal of AI in Healthcare and Medicine 1.1 (2021): 77-116.
8. Gadhiraju, Asha. "Empowering Dialysis Care: AI-Driven Decision Support Systems for Personalized Treatment Plans and Improved Patient Outcomes." Journal of Machine Learning for Healthcare Decision Support 2.1 (2022): 309-350.
9. Tamanampudi, Venkata Mohit. "Automating CI/CD Pipelines with Machine Learning Algorithms: Optimizing Build and Deployment Processes in DevOps Ecosystems." Distributed Learning and Broad Applications in Scientific Research 5 (2019): 810-849.
10. J. Singh, “Understanding Retrieval-Augmented Generation (RAG) Models in AI: A Deep Dive into the Fusion of Neural Networks and External Databases for Enhanced AI Performance”, J. of Art. Int. Research, vol. 2, no. 2, pp. 258–275, Jul. 2022
11. S. Kumari, “Cloud Transformation and Cybersecurity: Using AI for Securing Data Migration and Optimizing Cloud Operations in Agile Environments”, J. Sci. Tech., vol. 1, no. 1, pp. 791–808, Oct. 2020.
12. Sangaraju, Varun Varma, and Senthilkumar Rajagopal. "Applications of Computational Models in OCD." In Nutrition and Obsessive-Compulsive Disorder, pp. 26-35. CRC Press.
13. Tamanampudi, Venkata Mohit. "A Data-Driven Approach to Incident Management: Enhancing DevOps Operations with Machine Learning-Based Root Cause Analysis." Distributed Learning and Broad Applications in Scientific Research 6 (2020): 419-466.