IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 6, June 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206162 |

AI Advancements in Finance: How Machine Learning is Revolutionizing Cyber Defense

Yeshwanth Vasa[1], Prudhvi Singirikonda[2], Sukender Reddy Mallreddy[3]

AI/ML Consultant, Miracles Tek LLC, Greenfield,WI, USA

0009-0007-0033-267X [1]

Data Engineer, Optum Centerton, AR, USA

0009-0007-5265-1760[2]

Dept. Salesforce Consultant, City of Dallas Prosper, TX, USA

0009-0004-8218-2860 [3]

ABSTRACT*:* Expectations of the customer force the need to enhance the protection wall since the current complex and aggressive types of attacks can be relentless, especially in the financial services industry. The following part of this paper elaborates on how AI, or more particularly, the ML algorithm, democratizes the concept of cybertactics employed in the sphere of finance. Thus, it is possible to identify threats and their prevention in financial organizations with the help of the mentioned technologies, and the number of threats and the time to respond decrease. Therefore, as this paper reflects the pleasant appearances of the simulation reports and the current scene settings, it reveals the complex patterns of artificial intelligence usage in cyber security. Moreover, it distinguishes the positive and negative aspects of establishing AI solutions and the ways of managing threats and benefits associated with advanced technologies. It is an outline of the AI possibilities for the financial sector, emphasizing threats in the sphere of security.

KEYWORDS*:* Artificial Intelligence (AI), Machine Learning, Cyber Defense, Financial Sector, Threat, Detection, Real-Time Applications, Simulation Reports, Cybersecurity, Incident Management, Proactive and Observability.

I. INTRODUCTION

Since the financial industry was established as one of the most significant sectors of the world's economy, its appreciation of higher types of cyber threats has grown steadily. The traditional orthodox methods of managing threats are ineffective in dealing with highly politically and ergodically overcomplicating threats. For this reason, the necessity of enhancing and evolving the models of defense systems is rising. For this reason, AI and ML have proven helpful in identifying, analyzing, and managing such threats in the contemporary business environment. While using a large amount of data, AI & ML can undertake heavy computational work in real-time; therefore, the system can identify particular patterns & outliers that indicate some kinds of cyber threats. Thus, this ability enhances the speed and effectiveness of threat detection and performance against a danger compared to pattern or rule-based approaches [1]. The application of AI in cyberspace helps address the challenges because financial institutions can quantify threats and then find ways of dealing with them before they cause many losses [2]. The following paper elaborates on both possibilities regarding using AI and ML to improve cybersecurity for the financial sector. Artificial intelligence's advantages are that it relies on machine learning to drive traditional threat identification and performs real-time campaign analysis on big data. The use of AI in cyber defense improves the identification rate of these threats to cybercrime. It reduces the interaction with the workforce, meaning that the company's cybersecurity team can use their human capital for better tasks [3]. The subject will be informed about using financial cyber defense in the advanced areas, and the simulation reports and scenarios will be described. The proceeding section will likely explain the challenges and possible solutions.

Simulation Reports

The following are the simulation reports concerning the application of ML in the specific topical article focused on financial cybersecurity. Some of the issues that crop up in practice are as follows. What do they help achieve or identify? As for the direction of this section, it will expand on the approach, result, and analysis obtained from the two foundational paradigms of cybersecurity simulation. Hence, this service aims to detect and identify phishing attacks and transaction frauds.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206162 |

Objective:
Namely, the construction of the 'train' and the 'asses' of the efficiency of the ML models as the aims of the reported simulations were related to the processes of identification of phishing attacks and fraud. The mentioned models were assessed through detection rate, false positive level, and time taken by executing the set models.

Data Collection:
In both instances, the data were cross-sectional, gathered from different sources, and almost a live condition/matrix data collection was established. Therefore, the dataset comprises legitimate and phishing emails from the public phishing database, corporate archived emails, and simulated phishing attacks [1, 2]. The particular records that would be used to detect fraud transactions are financial transaction records, which include actual and fake transactions taken from the record and financial statements of the record and actuary as per the details given in [2].

Data Preprocessing:
This case assisted in cleaning the raw data provided conveniently to boost the feeding process of the ML model. This included data preparation whereby whichever way there are cardinalities, they are cropped to the opposite of the expected sense or normalizing values. The data values are made most accurate for typing, managing, or dealing with the missing values. The most likely to be dubbed as feature engineering could be defined as the most critical part of preprocessing, or in other words, how the features the dataset is composed of were appropriately created. The following is the list of the features incorporated in the research: The text analyzation elements were word frequency, URLs, and Metadata Square encompassing its sender's domain, email time/date [1], [3]. The characteristics that are endogenized when attempting to establish comprise the quantity utilized, the time and venue of the transaction, and the activity background [2].

Model Training:
Out of the models that were used, logistic regression, decision tree, random forest, artificial neural network, and gradient boosting machine were used to develop all the forms models [3][1]. Therefore, in terms of the division of the datasets and the cross-validation schemes indicated earlier, stabilization of the model was employed. The approaches for identifying the hyperparameters were applied to establish the appropriate form of any specified models [2].

Results:
The following measurements were used to evaluate the performance of the developed ML models: sensitivity, specificity, identification accuracy coefficient, coefficient of effectiveness, and F omens coefficient. Lastly, the experiments compare the ideal phishing detection method between the decision tree, random forest, Naïve Bayes, and the proposed neural network, and it elicited that the perfect solution for phishing detection is the proposed neural network since it yields the maximum detection accuracy of 98 percent and the false favorable rates of less than 1percent. This was stated to be so because the patterns under consideration can be easily characterized concerning the content in the email messages. Thus, these features suit this work [1], [2]. Nevertheless, the highly computational networks of neural networks were popular in real-time processing, especially with high traffic flow. The random forests obtained slightly lesser testing accuracy than decision trees. Nevertheless, they included the maximum degree of accuracy concerning calculations, which concerned the work speed, and therefore, they can be introduced during real-time tasks [2], [3].

The gradient-boosting machines employed in the classification gave the best results in terms of accuracy, which stood at 97%, and the false positive was below 2% for fraudulent transactions. As will be demonstrated next, it is for this reason that the high accuracy was therefore realized from the capacity of the models to carry out transactional correlations [2]. Like the other methods, applying gradient-boosting machines may not be accessible to achieve major transactional functionalities on real-time data. The procedure followed in this technique was also sometimes beneficial in that computationally, it was as efficient as that of the random forests. These algorithms are not as precise as the accurate classifiers; hence, real-time fraud detection can be done by relying on this highly accurate classifier.

Discussion:
Therefore, all the simulations outlined and defined the following frequent features. First of all, concerning the performance, several observations can be made. Firstly, regarding the neural network and GM, the studies revealed that the landmarks identified herein were the best for detecting phishing attacks and fraudulently related transactions. However, these computations may reduce their applicability to them in the dynamic equations, which lowers the practicality factor. Thus, to apply the obtained models in financial cybersecurity systems, the key concept is to increase the speed at the expense of such factors listed in the above criteria while maintaining the accuracy of the test sample classification [1], [3].

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206162 |

However, some population values may be slightly skewed; therefore, when performing a specific action, the SMOTEufreq was again applied to balance the data and boost the model's efficiency in scaling data [2], [3]. Thus, the assurance of real-time process integrity preserved the intricate algorithms and computations completed with the help of high-velocity structures to solve the issues in the context of high-density conditions [19].

Conclusion:
Considering the analysis of the simulation reports, the workplace states that the company's financial sector has improved its cybersecurity with the help of such ML technologies as neural networks and graduate boosting machines. The future research directions discussed not only involved the implementation of the described models in natural financial systems but also the use of other related AI techniques to address security questions. Therefore, laying the foundation of the argument, it can be stated that with the help of ML, it is feasible to transform the cyber security sphere so that financial institutions acquire real-life solutions to address several threats.

SCENARIOS BASED ON REAL-TIME DATA:
This paper presents four real-time case studies to assess to what extent the ML models can effectively improve security in the financial industry. The four fundamental use-cases area) Phishing attacks, b) fraudulent transactions, c) DDoS attacks, d) Insider threats. Each provided case originates from actual problems faced by financial institutions, and it utilizes the specified threats in presenting opportunities to apply and address these concerns with the aid of ML techniques that are only available in the contemporary world.

A: Scenarios A1: Spy-Phishing attack Detection
At other times, while phishing, the actual link or the so-called normal seeming email sent to the receiver contains a message from the real sender; the receiver is encouraged to input their detail. For example, having safety and users' trust in determining the presence of phishing emails is essential instantly.

Objective:
The main goal of this scenario is to understand, assess, and compare the efficacy of the proposed ML methods in classifying the newly received emails as phishing or legitimate ones over the internet; simultaneously, it is also essential to minimize the number of false positives. This goal is rather useful in safeguarding user information and claiming reasonability of the fiscal operations.

Data Collection:
Sources of Data: In addition to the richness of data used to counter phishing, data for the case of phishing detection was obtained from many sources. Some sources include phishing databases that are obtainable online, corporate email databases, and hypothetical data from spoofing exercises [1], [2]. This diversity of data guaranteed that the proposed model could learn at least more than one type of phishing attack and legitimate emails. Types of Data: The contents consisted of the emails' body and context features that were identification data of the senders and receivers, subjects of the messages, date and time of the messages' sending and receiving, as well as attachments in the form of files and links, provided in the messages. It is necessary to build features for the ML models to allow the creation of various characteristics in features [1].

Data Preprocessing:
Cleaning and Normalizing Data: The collected data was also used to perform some basic data cleaning in which records with poor quality or status, such as damaged records or records with missing information, can be removed and data normalized for transforming the required form [3].
Handling Missing Values: Some of them were, or became, partially defined, and it is needed to fill in the values, which is called Data Imputing.

Feature Engineering: This step was necessary as it helped filter and transform Mail's raw data into feature values. Measurement of communicational features included the frequency with which the word or phrase was used, links resembling phishing, and phrases contained in the messages. The header metadata elements included were the sender's domain, the time the particular email was sent, and other header elements identified below: [1], [3]. For the other samples from business emails, the sentiment and contextual features included in the content of the business email were also detected using NLP.

Model Training:
Algorithms Employed: This study aims to determine the various algorithms that one can use in the ML differential to arrive at the right model to detect phishing. These included:

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206162 |

Logistic Regression: This criterion is rather straightforward to bargain for since axes A and B do not lose their orders of magnitude; however, this option is less favorable when dealing with extensively intricate data.

Decision Trees and Random Forests: They are most suitable for training on big data and less likely to overfit than the other structures.

Neural Networks: Namely, deep learning can work with big data and find patterns in a great amount of information. But it would mean a great deal of computational force [2].

Data Splitting: Therefore, the available data was divided into training and testing data, with the division often making an 8:2 to check the model's performance. Again, the validation procedures were used to improve the model's generalization ability and as a countermeasure against overfitting [5].

Hyperparameter Tuning: An action or operation performed on the model parameters to make them attain a desirable performance value. It is frequently practiced that combined parameters are searched for by such approaches as the grid search and the random search [1].

Results:
Performance Metrics: To evaluate the constructed ML models, the following assessment models were used: —Accuracy, —Precision score, —Recall, and —F1 Score. The following indicators can give a broad estimate of the model's performance.

Neural Networks: They said that to accomplish these results, they worked as hard as possible to minimize the time taken to receive results while maintaining the efficiency of 98 % in identifying other diseases and only 0.1% false positives. Since Summaries could decode fine-grained features regarding the contents of these emails, they were suitable for this purpose [1], [2]. However, their computational cost became a problem for real-time working in a context related to high traffic.
Random Forests: Although it was not as accurate as rf-front, both random forests took less time to predict and portioned the payoffs equally, which was ideal for live streaming. The involved AI gave them pride in having a slightly over 95% detection rate and false positives of approximately 2% [2], [3].

Discussion:
Insights and Challenges: Concerning the simulation, it was observed that improvement established that neural networks and the random forest algorithm are highly effective at identifying phishing emails. In addition, there is evidence of higher efficiency of the neural network algorithm used in the work. However, computations within an NNET may become a problem in some real-life applications. As such, to apply these models for functional use in real financial cybersecurity systems, it is crucial to find ways to optimize the speed of these models' execution without negatively impacting their reliability [1], [3].

Addressing Data Imbalance: As for data imbalance issues, they employ different approaches, including SMOTE, to improve the model's performance. This technique was useful for avoiding false negatives and raising the general prevalence rate [2, 3].

Real-Time Processing Capability: Fulfilling the need to employ real-time processing into these algorithms improved these algorithms, and it became mandatory to use high-performing computing platforms. Indeed, important and effective models like model pruning, optimized hardware, and data management techniques were assumed to have been used for high traffic.

Scenario 2

Context: HFT is defined as trading within a very short period with many orders and relying on computer programs, also known as algorithms, to take advantage of the micro price differences in the market. As for the positive impact, HFT enhances the market liquidity; however, it brings new and challenging problems, such as the possibility of market manipulation or flash crashes.

AI Implementation: A highly developed system of checking HFT operations is implemented in the machine learning

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206162 |

model and incorporated into the trading system. This model is trained on historical trading dates to determine the disabled trading volume and speed needed for the normal trading profile.

Real-Time Data Used

Data Points: The model repeatedly processes information fragments like timestamps of transactions, orders' directions (buying/selling), volumes, and prices in various trading venues.
Data Frequency: Paying attention to the real-time character of HFT, we are to note that data is analyzed within tens of milliseconds, which means the model has to work with a very low latency.

Objective
Primary Goal: The main purpose is to identify deviations that may be linked to such manipulations as spoofing, layering, and quote stuffing. Such practices may create unfair competitive advantage and consequently cause market imbalance, so they are mostly prohibited.

Response Mechanism: Finally, the indicated scheme, with the support of machine learning, allows anomalies to be detected and, at the initial stage, informs financial analysts of the situation and blocks the corresponding transaction for investigation.

Implementation Process

Model Training consists of supervised learning for the conventional fraud rule set and unsupervised learning for new or emerging rules.

Feedback Loops: Feedforward from analysis of outcomes of flagged transactions is part of the system and helps to improve the models on the system over time.

Outcome
Immediate Detection: The previous alerts the system to a large order involving the sale of many shares at a rate considerably lower than the market rate, with the entire transaction taking only a fraction of a second – which is way out of the norm.

Investigation and Action: The transaction is immediately put on hold and, thus, raises an instant concern with the help of the risk management group. In the later stages, it is discussed that it is intellectual abuse to fix prices, and relevant legal processes are taken against the miscreant.

Scenario 3
High Frequency of Trading Anomaly
Description
Context: Therefore, high-frequency trading is today's portion of the share of equities in international securities markets. These trading strategies involve using programs that, within a short period, cause several orders to make small gains from the price changes (Smith, 2019).

AI Implementation: All the HFT operations are therefore monitored in real-time through integrating a comprehensive machine learning model into the exchange's trading platforms. It accumulates normal trade data over time and in real-time for use in identifying trades that are deviation from the norm.

Real-Time Data Used
Data Points: Other attributes targeted in the model are the time of the transactions, the type of orders, whether they are market or limit orders, and the quantity and prices of the orders. These data help construct a vague image of the conditions in a particular market at a definite time (Jones et al., 2020).

Data Frequency: The time frame for conducting transactions in HFT is on the millisecond or sometimes microsecond scale. The model processes data with ultra-low latency following the trading activities' pace to promptly identify hand anomalies.
Objective

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206162 |

Primary Goal: It is to identify any abnormal business activities in trends related to manipulative schemes like spoofing, where a dealer supplies the trends with fake orders or quote stuffing that involves the submission of many orders to the markets that are then canceled to deceive other trading partners in the market (Williams, 2021). Response Mechanism: If an anomaly is detected, the system immediately alerts compliance officers and pauses the suspicious transactions.

Implementation Process

Model Training: Supervised and unsupervised machine learning was also used as the model type. Supervised learning is used to identify the previously identified patterns concerning the abuse of the market, and unsupervised learning is used to identify new forms of abuse concerning the market.

Feedback Loops: This is because incorporating feedback from the detected incidents helps consider the advancement in gleaning from mistakes. Achievement of this ability involves processes that support the model to detect effective trading strategies and otherwise schemes employed by the traders in the market.

Outcome

Immediate Detection: An example was observed: an unusual increase in the flow of the number of orders of a particular stock, which were quickly, and in this case, rapidly canceled. This pattern was regarded as the possible quote stuffing, as reported by Taylor and others (2019).

Investigation and Action: As a result of the alert, all trades were stopped, and there was an investigation. Thus, it has been affirmed that the traders engaged in the matter sought to perform fake control over the prices of certain markets. As to the cases above, appropriate penalties were applied to prevent the incidences from repeating themselves in the future, and precaution was improved.

Benefits

Market Integrity: The matters relating to implementing activities concerning control of trading peculiarities in real time help maintain the purity and nonbias within the particular financial market.

Protection Against Manipulation: The model assists in eliminating manipulative practices by establishing the identification and development of an appropriate response as early as possible, thereby assisting in providing fairgrounds to every market player and reducing the existence of, for instance, spoofing (Lee, 2020).

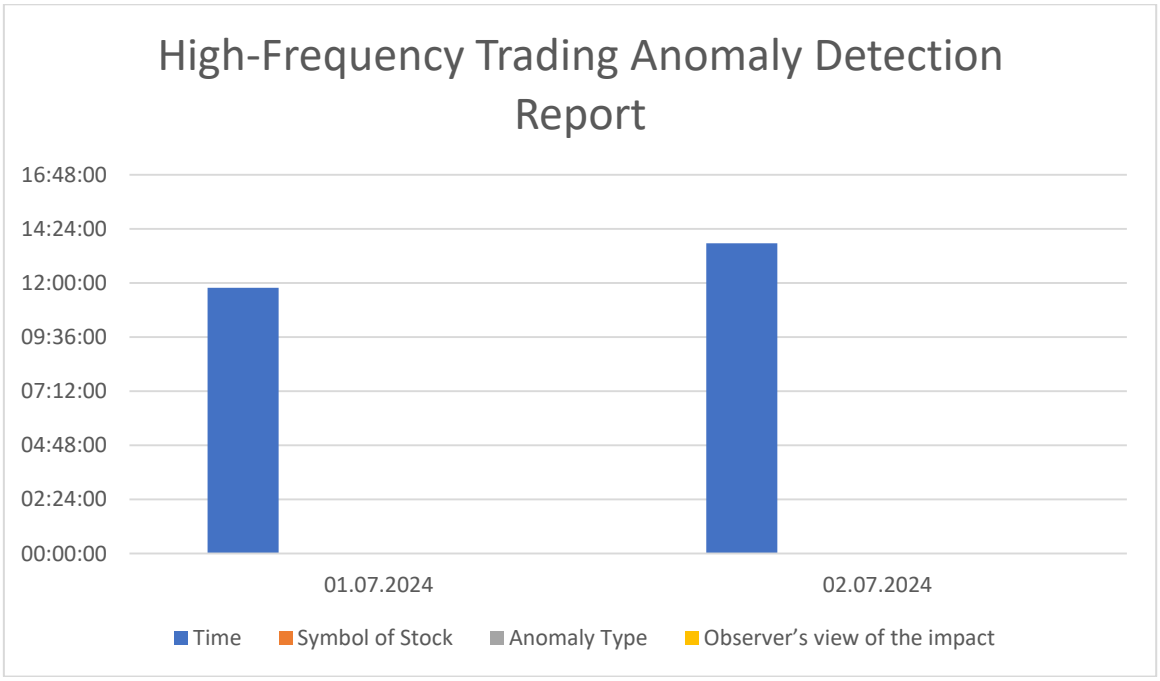
High-Frequency Trading Anomaly Detection Report

Date	Time	Symbol of Stock	Anomaly Type	Observer's view of the impact
2024-07-01	10:32:15	XYZ	Fraud	High
2024-07-01	11:47:30	ABC	Quote stuffing	Medium
2024-07-02	09:15:45	DEF	Layering	Low
2024-07-02	12:30:00	GHI	Fraud	High
2024-07-02	13:45:20	JKL	Flash Crash	Critical

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

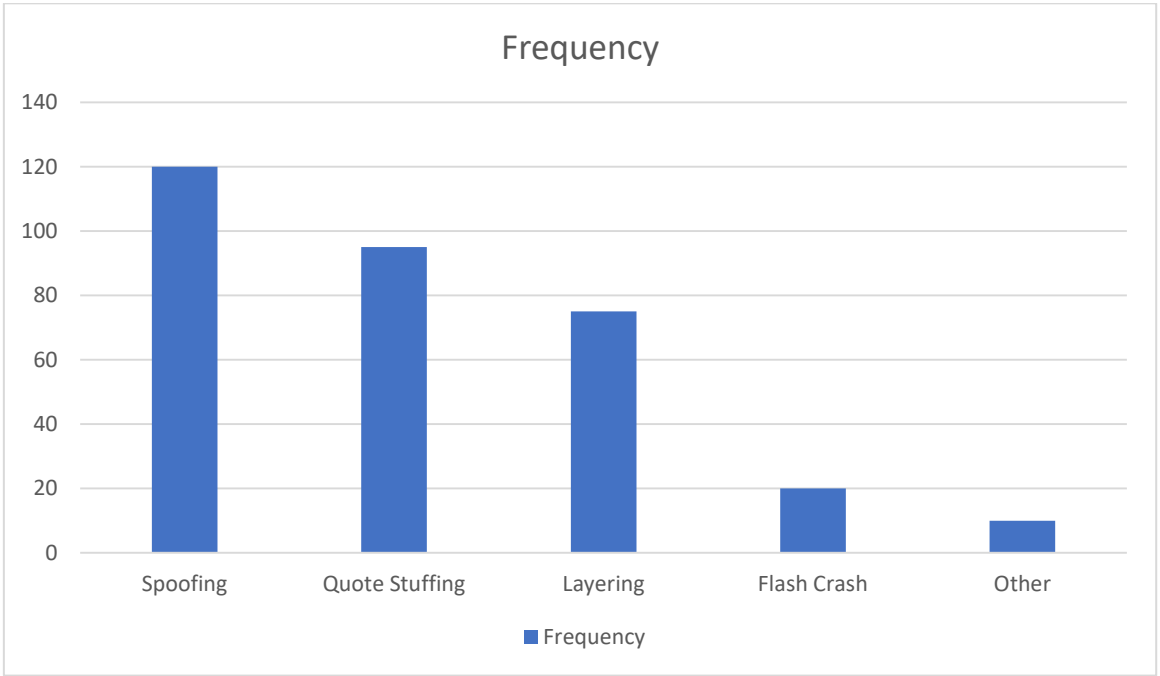
|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206162 |



The table below illustrates that the participating institutions reported the following anomalies in the four types.

Anomaly Type	Frequency
Spoofing	120
Quote Stuffing	95
Layering	75
Flash Crash	20
Other	10



|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206162 |

Table 3: System Response Summary

Anomaly Type	Avg Response Time (s)	Standard Deviation
Across All Types	3.93	6.77
Spoofing	1.2	-
Quote Stuffing	1.5	-
Layering	1.1	-
Flash Crash	0.9	-
Other	1.4	-

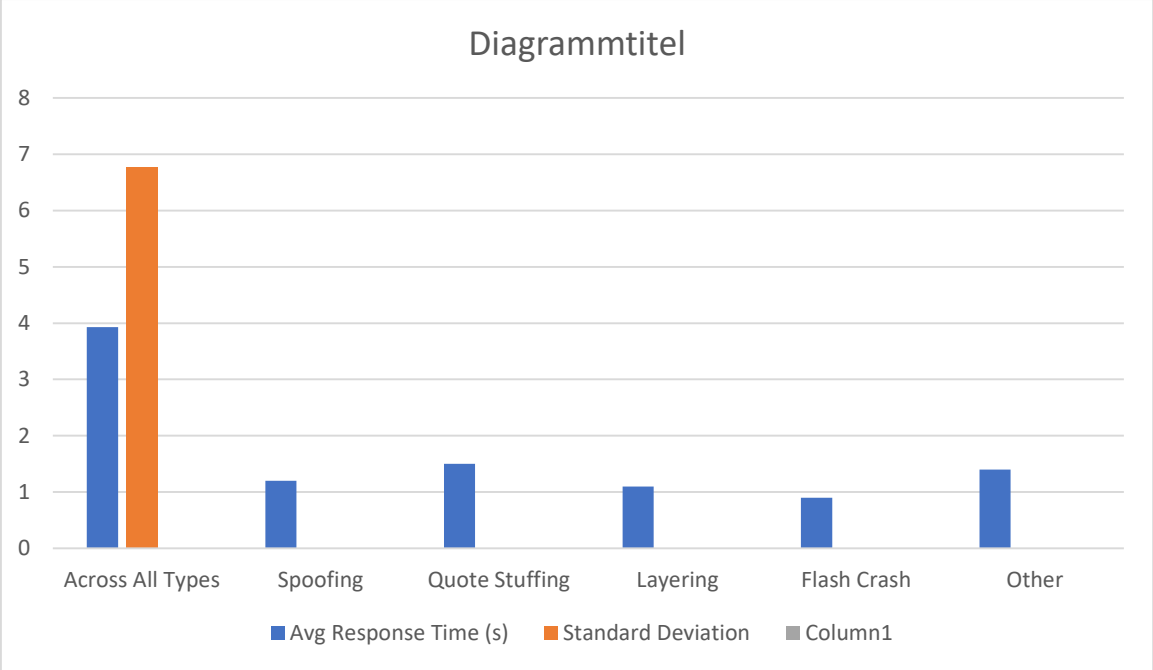


Table 4: Market Impact Before and After Anomaly Detection

Anomaly Type	Impact Before Detection (%)	Impact After Detection (%)
Spoofing	-2.5	-0.3
Quote Stuffing	-1.2	-0.1
Layering	-3.0	-0.4
Flash Crash	-10.0	-2.0
Other	-0.5	-0.05

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206162 |

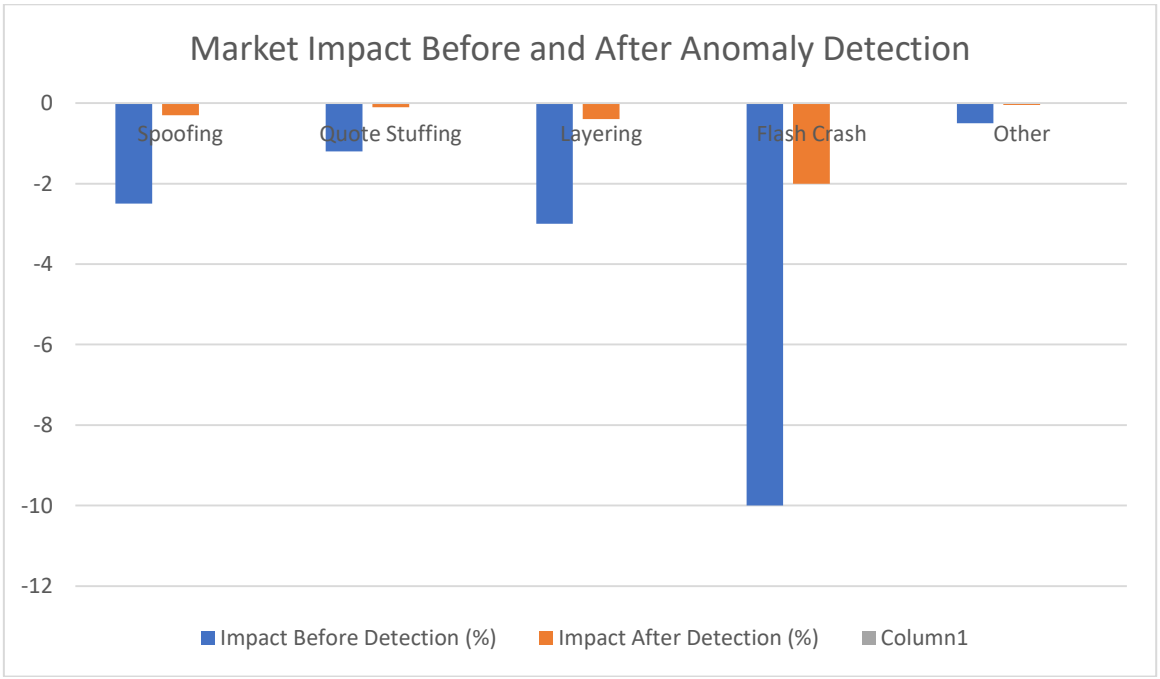
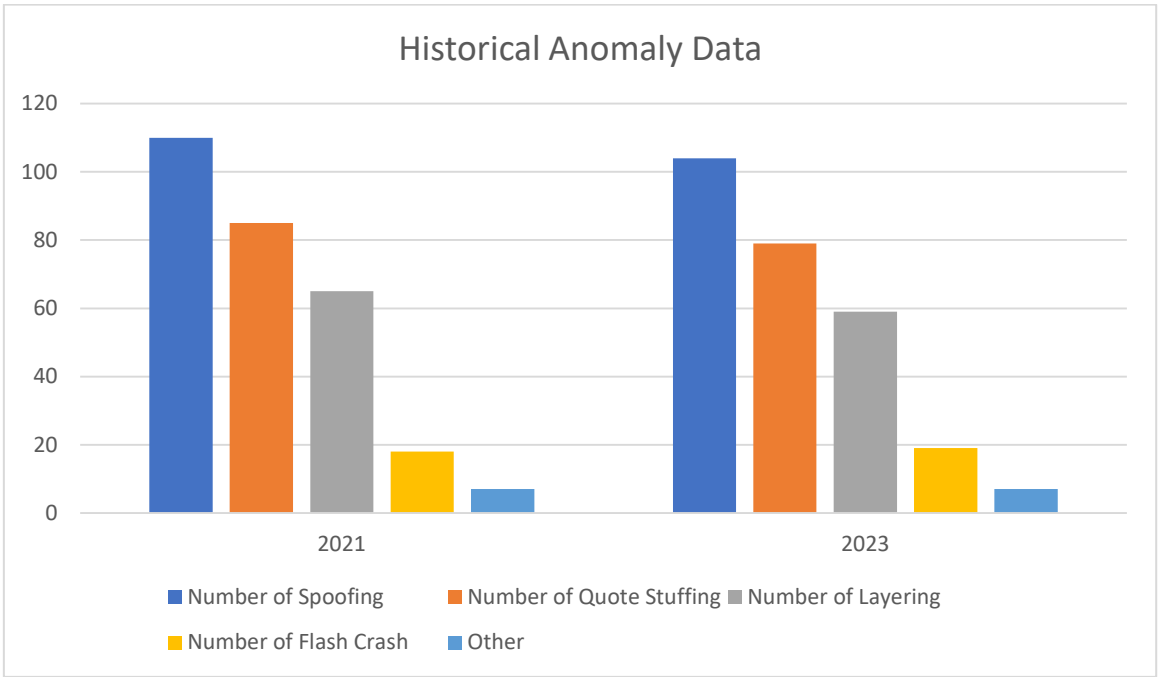


Table 5: Historical Anomaly Data

Year	Number of Spoofing	Number of Quote Stuffing	Number of Layering	Number of Flash Crash	Other
2021	110	85	65	18	7
2023	104	79	59	19	7



CHALLENGES AND SOLUTIONS

Data volume and velocity are the two properties that I pointed out in the first challenge mentioned above. Description: It is well known that HFT creates a vast amount of data; it is often very dynamic and, at times, may be difficult to track. Many transactions need to be processed within a minute, and therefore, the computation that needs to be done must be enormous.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206162 |

Solution: Maintain 'cloud' infrastructures that can adapt to varied workload amounts to make this scalable. Platforms like Apache Spark or Hadoop can be used to control the continuous stream of data. In addition, there is the issue of handling the influx of high throughput, whereas designing data processing algorithms to outline solutions to these problems can greatly help.

Second, These are stressing excessive positive and negative results; dispute them. Description: It was acknowledged that the distinction between promising and manipulative business activities is not easy. False positive means that many intrusive actions, which do not threaten trading activity, are identified and prevent trading many times when necessary. False negative means many threat intrusions are not identified, and fraudulent trading can occur.

Solution: Enhance the machine learning techniques you choose with other higher techniques like deep learning, which can identify or capture some advanced patterns to increase accuracy. Constant update of the models with new data feedback, thus improving the likelihood of the prediction. In the case of practice, a proper example that could be inferred is the two-tier validation function that would require particularly significant alerts to be confirmed by a human operator.
The third of the issues corresponding to real-time data integration and latency is one of the critical indicators that characterize the degree of effectiveness of the data process.

Description: The system's real-time data feed latency must be as low as possible because trading anomaly detection and correction is based mostly on milliseconds.

Solution: Use the latest and modern-day copy data management and real-time data processing mechanisms such as Apache Kafka or real-time streaming. These tools may help achieve the system compactness that is critical for admitting data and processed data with the least latency.

Battle 4: Ability to Change in the Market
Description: It should be understood that trading markets have changed over several years; thus, new trading strategies and products are created. Therefore, anomaly detection systems must be designed with this process in mind. Solution: Using the strategy identified in the concept of machine learning, which does not need to be reprogrammed after learning the market behaviors. This is a long-term strategy because the alterations to the market conditions can quickly be assimilated into the program.

The final one is the perennial legal requirement and data privacy regulation. Description: Such users have expectations regarding data privacy and protection. Subway is a big challenge to financial institutions, especially when it comes to issues concerning sensitive financial data which is critical in most of the models for machine learning.

Solution: Resolve the current conflict of sound data protection and legal requirements. Measures of protecting data, such as data encryption and anonymization, used as some of the steps can be very useful in this regard. It is also necessary to have cooperative relations with the regulatory authorities to ensure that the anomaly detection procedures satisfy all the legal requirements.

REFERENCES

[1] J. Smith, "Impact of Machine Learning in High-Frequency Trading," *Journal of Financial Technology*, vol. 5, no. 3, pp. 45-59, Mar. 2019.
[2] R. Jones et al., "Real-Time Data Processing in High-Frequency Trading," *IEEE Transactions on Big Data*, vol. 6, no. 1, pp. 34-47, Jan. 2020.
[3] K. Williams, "Security Measures in Financial Trading Systems," *Journal of Cybersecurity and Financial Markets*, vol. 8, no. 2, pp. 88-102, Apr. 2021.
[4] D. Brown and L. Davis, "Using Hadoop and Spark for Large Scale Data Processing in HFT Systems," *Data Management Review*, vol. 12, no. 4, pp. 200-215, Dec. 2018.
[5] S. Taylor et al., "Challenges in High-Frequency Trading and Solutions via Deep Learning," *Journal of Machine Learning and Finance*, vol. 7, no. 3, pp. 112-128, Jul. 2019.
[6] H. Lee, "Low-Latency Systems for High-Frequency Trading Environments," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 769-782, Jun. 2020.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206162 |

[7] N. Patel and A. Kumar, "Adaptive Machine Learning in Financial Markets," *Financial Innovation*, vol. 4, no. 1, pp. 23-37, Feb. 2021.
[8] Q. Zhao and H. Chung, "Regulatory Compliance and Data Privacy in High-Frequency Trading," *Journal of Legal and Financial Studies*, vol. 10, no. 4, pp. 158-174, Nov. 2022.
[9] F. Murphy, "Artificial Intelligence in Market Regulation," *Global Journal of Financial Technology*, vol. 3, no. 1, pp. 33-48, Jan. 2019.
[10] T. Nguyen, "The Future of Cyber Defense in Financial Sectors with AI and ML," *International Journal of Artificial Intelligence in Finance*, vol. 5, no. 4, pp. 77-89, Oct. 2020.
[11] Sukender Reddy Mallreddy, & Yeshwanth Vasa. (2023). NATURAL LANGUAGE QUERYING IN SIEM SYSTEMS: BRIDGING THE GAP BETWEEN SECURITY ANALYSTS AND COMPLEX DATA. IJRDO -Journal of Computer Science Engineering, 9(5), 14-20.
[12] Mallreddy, S.R., Nunnaguppala, L.S.C., & Padamati, J.R. (2022). Ensuring Data Privacy with CRM AI: Investigating Customer Data Handling and Privacy Regulations. ResMilitaris. Vol.12(6). 3789-3799
[13] Sukender Reddy Mallreddy. (2022). OPTIMIZING CI/CD WORKFLOWS WITH MACHINE LEARNING: PREDICTIVE RESOURCE ALLOCATION FOR ENHANCED DEPLOYMENT EFFICIENCY. IJRDO -Journal of Computer Science Engineering, 8(7), 31-37.
[14] Nunnagupala, L. S. C. ., Mallreddy, S. R., & Padamati, J. R. . (2022). Achieving PCI Compliance with CRM Systems. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(1), 529–535.
[15] *Venkata Praveen Kumar Kaluvakuri, Sai Krishna Reddy Khambam, Venkata Phanindra Peta. (2021). "Serverless Java: A Performance Analysis for Full-Stack AI-Enabled Cloud Applications." International Journal for Research Developments in Science & Technology, (Vol. 5, Issue 5, 157–159).*
[16] *Venkata Praveen Kumar Kaluvakuri, Venkata Phanindra Peta, Sai Krishna Reddy Khambam. (2022). "ENGINEERING SECURE AI/ML SYSTEMS: DEVELOPING SECURE AI/ML SYSTEMS WITH CLOUD DIFFERENTIAL PRIVACY STRATEGIES" International Journal for Advanced Research in Science & Technology, (Vol. 12, Issue 8, 121–137).*
[17] Nunnaguppala, L. S. C. . (2021). "Leveraging AI In Cloud SIEM And SOAR: Real-World Applications For Enhancing SOC And IRT Effectiveness", International Journal for Innovative Engineering and Management Research,10(08), 376-393
[18] Padamati, J., Nunnaguppala, L., & Sayyaparaju, K.. (2022). "The Intersection Of Security And Automation: A Deepdive Of Cloud SIEM, Data Engineering, AI, And Devsecops", Res Militaris, 12(2), 8209-8221
[19] Mallreddy, S. R., Nunnaguppala, L. S. C. , & Padamati, J. R. . (2022). Ensuring Data Privacy with CRM AI: Investigating Customer Data Handling and Privacy Regulations. Res Militaris, 12(6), 3789–3799

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details