International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I6P110

Volume 72 Issue 6, 72-79, June 2024

Original Article

How Real-Time Streaming Helping Fraud Detection for Trade Clearing Firms

Prabhu Patel

Fellow, IETE, New Delhi.

Corresponding Author : prabhu.patel@hotmail.com

Received: 26 April 2024 Revised: 29 May 2024 Accepted: 08 June 2024 Published: 19 June 2024

Abstract *- The application of Time-Series Analysis and Fraud Score Calculation as essential elements of clearing organisations' fraud detection systems is investigated in this paper. Using sequential data point analysis and numerical scoring of transactions, these analytical methods provide proactive ways to identify and reduce fraudulent activity. Through Fraud Score Calculation, clearing companies may quickly detect high-risk transactions and prioritise resources by utilising statistical methodologies and machine learning algorithms. In order to preserve market integrity, Time-Series Analysis simultaneously makes it possible to identify minute patterns and trends in transaction data, which paves the way for predictive modelling and proactive intervention. The results highlight how crucial these analytical skills are for negotiating the intricacies of the financial markets and avoiding possible dangers. On the other hand, clearing companies are better able to detect fraud, reduce losses, and maintain customer confidence thanks to the combination of Time-Series Analysis and Fraud Score Calculation.*

Keywords *- Real-Time Data Streaming, Fraud detection, Trade clearing firm.*

1. Introduction

Every transaction in the finance industry has the potential to be profitable as well as dangerous, as it sits at the nexus of innovation and risk. According to Lokanan, M. E. (2023), trade clearing companies are the gatekeepers of financial integrity in this ever-changing market, responsible for both protecting against fraud and guaranteeing the seamless settlement of trades. These companies now approach fraud detection in a completely different way thanks to real-time streaming technology, which provides never-before-seen possibilities for swifter and more accurate identification and prevention of illegal activity (Hassan & Mhmood, 2021).

The viewpoints and ideas of numerous writers who have investigated the connection between fraud detection in trade clearing businesses and real-time streaming are at the forefront of this paradigm change. These authors critically examine the implications of real-time streaming technology for the financial industry while illuminating the technology's disruptive potential through their research and analysis.

Shah (2021) emphasises the significance of real-time streaming technologies in augmenting the responsiveness and agility of fraud detection systems. According to the author, trade clearing companies can quickly detect and deal with fraudulent activity by evaluating data streams in real time, which reduces potential losses and maintains market integrity. According to Carcillo et al. (2018), real-time streaming has many benefits in terms of speed and immediateness, but it also comes with hazards and complications that need to be properly considered. In order to effectively prevent fraud, she highlights that trade clearing organisations must strike a balance between real-time detection and strong risk management measures. Additionally, Habeeb et al. (2019) note that real-time streaming has the potential to improve fraud detection capabilities significantly, but they also emphasise the significance of combining advanced analytics with human knowledge to extract actionable insights from real-time data streams efficiently.

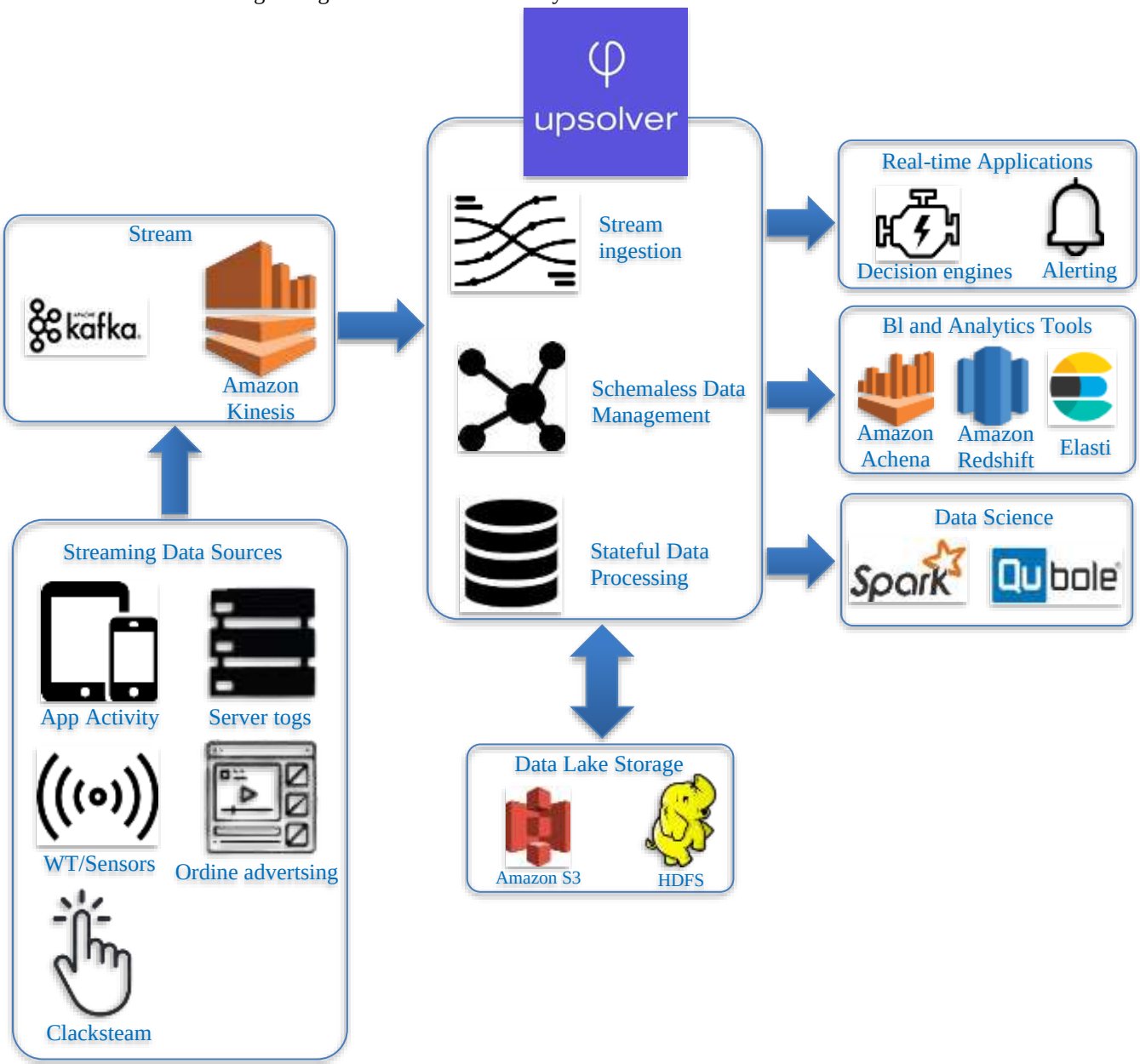
These opposing points of view make it clear that there are trade-offs and complexity involved in using real-time streaming technologies for fraud detection in trade-clearing organisations. Even though real-time streaming is incredibly quick and responsive, there are a number of things to keep in mind, including algorithmic bias, data protection, and regulatory compliance. The study looked at Time-Series Analysis and Fraud Score Calculation to investigate fraud detection for clearing firms. These techniques show two different ways to identify fraud, each with special benefits and insights.

2. Real-Time Streaming Technology

Real-time streaming technology is a crucial element of innovation in the field of fraud detection and operational efficiency for trade-clearing organisations (Javaid et al., 2022). According to Cao et al. (2019), this technology allows for the uninterrupted processing and analysis of data as it

moves through the system, giving trade clearing firms unparalleled speed, precision, and flexibility in responding to changing market circumstances and new risks. Real-time streaming technology fundamentally transforms the data handling process for trade clearing organisations, replacing old batch processing methods with a more dynamic and adaptable approach to data analysis (Rettig et al., 2019).

The core of real-time streaming technology resides in its capacity to handle data streams instantly, enabling immediate identification of anomalies, patterns, and trends. Trade clearing firms obtain immediate and valuable information about market trends and growing fraudulent activities by utilising real-time data from various sources such as market feeds, transaction logs, and social media streams (Fedoryszak et al., 2019). Stream processing technologies like Apache Kafka, Apache Flink, and Apache Spark Streaming are crucial in this process. They allow for the efficient processing, filtering, transformation, and aggregation of streaming data with little delay and high data processing capacity (Branco et al., 2020). The capacity to process data in real time enables trade clearing organisations to promptly identify and address fraudulent actions, thereby reducing possible financial losses and maintaining the integrity of the market.



Modern streaming architecture (source; uplover whitepaper, 2019)

The journey of streaming data from its source to its use in real-time applications, BI analytics tools, and data science platforms is a complex process of vital importance in the complex world of contemporary financial markets. First of all, streaming data comes from a variety of sources, including social media streams, sensor networks, market feeds, and transaction records. The foundation of real-time analytics in trade clearing organisations is this raw data, which is frequently produced at a high rate of velocity and volume. It offers a constant flow of information that captures the dynamic character of financial transactions and market conditions.

Using stream processing technology, streaming data is transformed in multiple ways after it is sourced. In order to extract valuable insights and actionable intelligence, stream processing entails the real-time analysis and manipulation of data streams. At this point, technologies like Apache Spark Streaming, Flink, and Kafka are essential because they make it possible to analyse, filter, transform, and aggregate streaming data at a high throughput and low latency. Stream processing guarantees quick data processing and makes it easier to obtain real-time insights that influence trade-clearing organisations' decision-making.

The processed data streams are then ingested or incorporated into other platforms and systems for use after stream processing. The processed data streams are utilised by real-time applications, such as trading platforms and algorithmic trading systems, to facilitate prompt decision-making and trade execution. With the use of visualisation and analysis features offered by business intelligence (BI) analytics tools like Tableau, Power BI, or Looker, users may examine and evaluate streaming data to learn more about consumer behaviour, market trends, and operational performance. Furthermore, data science platforms utilise real-time data to do sophisticated analytics and modelling. They do this by utilising statistical methods, machine learning algorithms, and predictive analytics to find trends, identify abnormalities, and project future results. Trade clearing companies use this thorough procedure to leverage streaming data to improve real-time fraud detection, risk management, and decision-making, protecting the integrity and effectiveness of financial markets.

3. Fraud Detection Technology

Fraud detection technology is an essential aspect of every modern business's armoury, especially in industries like banking, where there is a high danger of fraudulent activity (Cherif et al., 2023). This technology includes a wide range of instruments, formulas, and procedures intended to detect, stop, and lessen fraudulent activity. A comprehensive analysis of fraud detection technology highlights its advantages and disadvantages, illuminating the effectiveness of this tool as well as the difficulties it presents for companies.

The capacity of fraud detection technology to analyse massive volumes of data in real time is one of its main advantages; it allows organisations to quickly and accurately spot suspicious trends and abnormalities (Habeeb et al., 2019). Sophisticated machine learning methods, including random forests and neural networks, have proven very effective at identifying fraudulent activity in a variety of fields. These algorithms are capable of analysing large, complicated data sets, such as network traffic, transaction logs, and user behaviour patterns, to find fraudulent activity that could otherwise go undetected (Abakarim et al., 2018).

Nevertheless, fraud detection technology has drawbacks even with its improvements. False positives, in which valid transactions are mistakenly reported as fraudulent, are a prominent problem that causes needless disruptions and disgruntled customers (Vassakis et al., 2018). The intricacy of fraud patterns by nature and the shortcomings of current algorithms in differentiating between legitimate and fraudulent activity can give rise to this problem. Furthermore, fraud detection systems are always faced with difficulty due to the dynamic nature of fraud strategies. In order to stay effective, these systems must constantly adapt to new threats (Saia & Carta, 2019).

Moreover, privacy and ethical issues are brought up by the use of fraud detection technology, especially in relation to the gathering and use of sensitive personal data. To maintain compliance with data protection regulations and protect individual privacy rights, businesses deploying fraud detection systems must manage regulatory requirements and ethical issues (Carcillo et al., 2018). Furthermore, there is a chance that algorithms used in fraud detection systems can unintentionally discriminate against specific persons or groups, producing unjust results and escalating already-existing socioeconomic imbalances. Vassakis et al. (2018) added that this is known as algorithmic bias. Thennakoon et al. (2019) emphasise how technology may significantly improve trading organisations' capacity for fraud detection. The authors outline how fraud detection algorithms have changed over time, moving from more complex rule-based systems to machine learning and artificial intelligence (AI) models. They stress how crucial it is to use real-time analytics and big data to identify and stop fraudulent activity in trading operations. This analysis highlights how important technology is in allowing proactive and flexible fraud detection techniques that are suited to the ever-changing financial markets.

Chouiekh et al. (2018) highlight the shortcomings and difficulties with the fraud detection systems that are currently in use. The authors draw attention to issues with false positives, which occur when valid transactions are reported as fraudulent, causing needless delays and inefficiencies in operations. Additionally, this brings out concerns about the bias and interpretability of models in machine learning

algorithms, which might compromise the efficiency and impartiality of fraud detection systems. This criticism emphasises how crucial it is to integrate fraud detection technologies within trading organisations while maintaining a balance between innovation and risk management. However, the effectiveness of fraud detection technology in stopping fraudulent actions and shielding companies from financial losses depends on resolving critical issues such as algorithmic bias, false positives, and privacy concerns. Businesses must critically evaluate fraud detection technology in order to comprehend both its advantages and disadvantages completely. Businesses can improve their fraud detection skills while guaranteeing justice, transparency, and regulatory compliance by utilising cutting-edge algorithms, implementing moral best practices, and encouraging interdisciplinary cooperation.

4. Streaming Analytics

A cutting-edge method of data processing known as "streaming analytics" is completely changing how companies use real-time data streams to their advantage. Fundamentally, streaming analytics entails processing fast data streams as they enter the system, allowing businesses to extract insightful information and make decisions instantly (Mohammadi et al., 2018). Data streams, which include transaction records, sensor readings, social media updates, and website hits, can be thought of as a constant flow of events that happen quickly. Streaming analytics is about handling this flood of data in real time before it hits the database (Zhang et al., 2018).

Unlike batch processing techniques that work with static datasets, streaming analytics is fundamentally able to handle data in motion; real-time insights are more important than ever in today's fast-paced digital environment, as information is created and consumed at a never-before-seen rate (Ali et al., 2018). Rather than waiting for data to build up in a database before analysis, streaming analytics processes data as it enters the application, enabling businesses to keep up with this fast-paced flow of information.

By utilising the power of real-time data insights, clearing firms can use streaming analytics to improve their fraud detection capabilities and achieve actual success (Fei et al., 2019). Clearing companies can reduce risks, increase operational efficiency, and prevent fraud by quickly analysing and responding to streaming data. Personalised e-commerce marketing, banking alerts, actuators integrated into tangible items, real-time fraud detection, data and identity security services, and sensor-generated data analysis are just a few of the businesses that use streaming analytics (Elsaleh et al., 2020).

Streaming analytics gives clearing firms the ability to monitor and analyse transaction data in real time, which helps them identify suspicious actions, patterns, and anomalies as they happen in the context of fraud detection (Kumar & Huang, 2020). Clearing firms are able to quickly detect fraudulent transactions, unauthorised access attempts, and other criminal behaviours by continuously processing data streams from many sources, including market feeds, transaction logs, and customer interactions (Ali et al., 2018). By adopting a proactive strategy for fraud detection, clearing businesses can limit risks and prevent financial losses immediately, protecting their reputation and guaranteeing regulatory compliance.

Furthermore, clearing companies can use dynamic and adaptive fraud detection tactics thanks to streaming analytics, which change as new risks and market conditions arise (Hilal et al., 2022). Clearing companies can leverage machine learning algorithms, anomaly detection strategies, and behavioural analytics models to discover novel fraud tendencies, uncover abnormalities that were previously undetected, and modify their detection tactics accordingly (Josyula, 2023). Being adaptable and agile is essential to fending off scammers who are always looking to take advantage of holes in financial systems.

Additionally, by enabling real-time integration of external data sources and contextual information, streaming analytics can improve the efficacy and accuracy of fraud detection (Habeeb et al., 2019). Clearing companies can obtain a more thorough grasp of the context of each transaction and more precisely detect suspicious activity by adding further insights to transaction data, such as customer profiles, transaction history, geolocation data, and market trends (Ikegwu et al., 2022). By taking a comprehensive strategy for fraud detection, false positives are decreased, detection rates are raised, and overall operational effectiveness is improved.

5. Fraud Score Calculation

Fraud Score Calculation is a critical weapon in the armoury of fraud detection systems, offering a quantifiable estimate of the likelihood that a certain transaction or behaviour is fraudulent. At its foundation, Fraud Score Calculation uses statistical approaches, machine learning algorithms, and domain-specific rules to analyse the numerous aspects and patterns connected with each transaction (Situngkir & Triyanto, 2020). The idea is to assign a numerical score to each transaction, indicating the level of suspicion or danger it represents.

$$\sum_{i=1}^{n} w_i \times f_i$$

The Fraud Score denotes the total fraud score linked to a particular transaction, signifying the degree of suspicion that is justified.

w_i indicates the weight given to every characteristic or attribute, indicating how significant a role it plays in predicting fraud.

f_i represents particular features or attributes of the transaction and denotes the value of each feature or variable.

This formula captures the idea of Fraud Score Calculation, with each parameter adding to the overall score based on its weighted importance and observed value. By giving suitable weights to various variables, organisations may prioritise the most relevant signs of fraudulent behaviour and adjust their fraud detection models to unique business contexts and risk profiles. However, the success of Fraud Score Calculation is dependent on a number of aspects, including feature selection and calibration, weight determination, and the development of threshold values for interpreting fraud scores (Ratmono et al., 2020). To achieve the best performance, a data-driven approach is required, which involves combining previous transaction data and domain expertise to uncover relevant patterns and correlations that indicate fraud.

A valuable tool for trading companies looking to strengthen their fraud detection systems and protect themselves from financial dangers is Fraud Score Calculation. Through the process of allocating a numerical score to every transaction, trading firms are able to effectively allocate resources, mitigate losses, and maintain confidence within their operational framework (Beneish & Vorst, 2022). By using statistical techniques, machine learning algorithms, and industry-specific regulations, trading companies are able to carefully examine transaction data in order to identify patterns, identify abnormalities, and highlight questionable behaviour that may be a sign of fraud.

Furthermore, trading businesses may remain ahead of developing fraud concerns and modify their strategies in response to changing market dynamics because of the agility and adaptability provided by Fraud Score Calculation (Haqq & Budiwitjaksono, 2019). Trading organisations should remain proactive against fraudsters by continuously monitoring transaction data and improving Fraud Score models in response to changing fraud strategies. Trading companies may effectively handle massive volumes of data by automating the examination and scoring of transactions using machine learning algorithms; this allows them to quickly spot fraudulent tendencies that could elude manual detection (Irwandi et al., 2019). By providing auditable records of fraud detection actions, this automated technique not only improves the efficiency and accuracy of fraud detection but also aids regulatory compliance efforts, reducing the risk to one's reputation and legal standing.

Conversely, Fraud Score Calculation is a critical component of efficient fraud detection techniques, providing organisations with actionable insights to manage risks and protect against financial losses. Organisations may improve their fraud detection skills and maintain confidence and integrity in their operations by implementing the formulaic approach indicated above in the face of an increasingly complex and dynamic threat landscape.

6. Time-Series Analysis

A potent statistical method for analysing and deriving conclusions from successive data points gathered over time is time-series analysis. In order to forecast, spot anomalies, and gain practical insights, time-series analysis essentially entails looking for patterns, trends, and relationships within a time-ordered collection; the data points in this analysis are expressed as a sequence of observations indexed by time, and this is captured in a formula (Mudelsee, 2019).

$$MA_t = \frac{1}{n}\sum_{i=0}^{n-1} x_{t-1}$$

MA_t symbolises the moving average at t.

n indicates how many data points are there in the window of the moving average.

x_{t-1} represents the time series' value at time t-i, where i varies from 0 to n-1

In Time-Series Analysis, moving averages are frequently used to reduce volatility and reveal underlying trends or patterns in the data. Moving averages give a more accurate representation of the overall trajectory of the data over time by averaging the values of the time series over a certain window of observations. Time-series analysis is a powerful tool that trading companies may use to strengthen their fraud detection systems and protect themselves from illegal activity. Time-Series Analysis allows trading organisations to identify complex patterns, trends, and anomalies that may be signs of fraudulent activity by examining successive data points over time (Fulcher, 2018). The utilisation of this analytical method for detecting fraud provides numerous advantages that are essential for managing the intricacies of financial markets and maintaining the integrity of the market. Trading firms can detect potentially fraudulent conduct by using Time-Series Analysis to proactively uncover small patterns and variations within transaction data (Chatfield & Xing, 2019). Trading companies can minimise financial losses and uphold trust in their operations by quickly identifying anomalies and setting baseline trends.

Additionally, Time-Series Analysis facilitates forecasting and predictive modelling, allowing trading companies to detect and stop fraudulent activity before it happens (Nielsen, 2019). Trading firms can determine possible fraud hotspots,

allocate resources accordingly, and put preventive measures in place by extrapolating future trends from historical data. By using a proactive approach, fraud detection skills are improved, and the negative effects of fraudulent activity on operations and financial performance are reduced. Time-series analysis also makes it easier to implement adaptive fraud detection procedures and continuous monitoring, which helps trading organisations keep ahead of emerging fraud techniques and quickly adjust to shifting market conditions (Silva et al., 2021). In the face of a constantly changing financial environment, this adaptability and agility are crucial for upholding market integrity and taking a proactive approach to preventing fraud.

However, time-series analysis is an effective method for deciphering and examining sequential data that has been gathered over time. Analysts can find patterns, trends, and linkages in time-ordered information that drive business insights and influence decision-making by using statistical approaches and mathematical models. Even though Time-Series Analysis has many useful applications in forecasting and prediction, robust and trustworthy outcomes necessitate careful examination of data assumptions, model selection, and interpretation. Time-Series Analysis will continue to be a vital component of predictive analytics and data-driven decision-making techniques as long as organisations gather and examine enormous volumes of time-series data.

7. Findings and Conclusion

In their efforts to improve fraud detection skills, clearing firms have made great progress with the use of Time-Series Analysis and Fraud Score Calculation. A critical analysis of the results shows that combining these analytical techniques provides a comprehensive plan to fight fraud successfully. First off, by putting Fraud Score Calculation into practice, clearing firms are given a methodical way to assess the risk involved in every transaction. Clearing corporations are able to effectively allocate their resources by use of a numerical score that is determined by a variety of features and behaviours, including transaction volume, frequency, and divergence from conventional patterns. As a result, they can concentrate on transactions that have higher fraud scores, which streamlines their efforts to detect fraud and guarantees prompt identification and intervention in high-risk operations. The utilisation of sophisticated statistical methods and machine learning algorithms augments the precision and efficacy of Fraud Score Calculation, permitting clearing companies to scrutinise transaction data in a thorough manner and identify minute irregularities suggestive of fraudulent conduct. By taking a proactive stance, clearing companies can minimise losses and maintain market integrity by staying ahead of possible risks in real time.

Furthermore, the integration of Time-Series Analysis gives clearing companies an effective tool for identifying underlying trends and patterns in transaction data over time. Through the examination of consecutive data points and historical trend analysis, clearing firms can get significant insights into the workings of fraudulent activity. Clearing businesses can detect patterns that deviate from expectations and predict fraudulent activities before they completely materialise, according to Time-Series Analysis. With the help of these predictive modelling capabilities, clearing companies may act proactively to reduce risks and uphold customer confidence in their operations. In an ever-changing financial world, clearing firms can protect themselves from potential financial losses and maintain market integrity by utilising Time-Series Analysis to improve their detection and prevention of fraudulent actions.

Additionally, the results imply that time-series analysis and fraud score calculation work well together to support ongoing surveillance and flexible fraud detection tactics. Clearing firms can remain ahead of new fraud strategies and quickly adjust to shifting market dynamics by doing real-time analysis of time-series data and upgrading fraud detection models accordingly. In an increasingly complex financial sector, this agility and adaptability are critical for upholding market integrity and taking a proactive approach against fraud.

The results highlight how crucial it is for clearing firms to use Time-Series Analysis and Fraud Score Calculation as essential elements of their fraud detection tactics. Through the utilisation of these analytical techniques, clearing companies can improve their capacity to identify and address fraudulent activity, reduce monetary losses, and uphold integrity and confidence in their operations. The application of Fraud Score Calculation and Time-Series Analysis will continue to be essential for negotiating the complexities of financial markets and protecting against possible dangers as clearing organisations continue to face new fraud threats.

On the other hand, clearing businesses' efforts to detect fraud have advanced significantly with the use of Time-Series Analysis and Fraud Score Calculation. With the use of these analytical techniques, clearing companies can effectively prevent fraudulent activity by identifying high-risk transactions quickly, allocating resources accordingly, and taking proactive measures to reduce risks. By proactively assigning numerical ratings to transactions, fraud score calculation helps to minimise financial losses and enable real-time fraud detection. In contrast, Time-Series Analysis gives clearing companies the ability to identify minute patterns and trends in transaction data, allowing for predictive modelling and proactive intervention to preserve market integrity.

References

[1] Youness Abakarim, Mohamed Lahby, and Abdelbaki Attioui, "An Efficient Real Time Model for Credit Card Fraud Detection based on Deep Learning," *Proceedings of the 12th International Conference on Intelligent Systems: Theories and Applications*, Rabat Morocco, pp. 1-7, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[2] Muhammad Ali et al., "Edge Enhanced Deep Learning System for Large-scale Video Stream Analytics," *2018 IEEE 2nd International Conference on Fog and Edge Computing*, Washington, DC, USA, pp. 1-10, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[3] Messod D. Beneish, and Patrick Vorst, "The Cost of Fraud Prediction Errors," *The Accounting Review*, vol. 97, no. 6, pp. 91-121, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Bernardo Branco et al., "Interleaved sequence RNNs for Fraud Detection," *Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, CA USA, pp. 3101-3109, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Shaosheng Cao et al., "Titant: Online Real-time Transaction Fraud Detection in Ant Financial," *arXiv*, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] Fabrizio Carcillo et al., "Scarff: A Scalable Framework for Streaming Credit Card Fraud Detection with Spark," *Information Fusion*, vol. 41, pp. 182-194, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[7] Chris Chatfield, and Haipeng Xing, *The Analysis of Time Series: An Introduction with R*, Chapman and Hall/CRC, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[8] Asma Cherif et al., "Credit Card Fraud Detection in the Era of Disruptive Technologies: A Systematic Review," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 1, pp. 145-174, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Alae Chouiekh, and EL Hassane Ibn EL Haj, "Convnets for Fraud Detection Analysis," *Procedia Computer Science*, vol. 127, pp. 133-138, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[10] Tarek Elsaleh et al., "IoT-Stream: A Lightweight Ontology for Internet of Things Data Streams and Its use with Data Analytics and Event Detection Services," *Sensors*, vol. 20, no. 4, pp. 1-22, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] Mateusz Fedoryszak et al., "Real-time event Detection on Social Data Streams," *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, Anchorage AK USA, pp. 2774-2782, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[12] Xiang Fei et al., "CPS Data Streams Analytics Based on Machine Learning for Cloud and Fog Computing: A Survey," *Future Generation Computer Systems*, vol. 90, pp. 435-450, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[13] Ben D. Fulcher, *Feature-based Time-series Analysis, Feature Engineering for Machine Learning and Data Analytics*, 1st ed., CRC Press, pp. 1-30, 2018. [Google Scholar] [Publisher Link]

[14] Riyaz Ahamed Ariyaluran Habeeb et al., "Real-time Big Data Processing for Anomaly Detection: A Survey," *International Journal of Information Management*, vol. 45, pp. 289-307, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] Ananda Putra Nindhita Aulia Haqq, and Gideon Setyo Budiwitjaksono, "Fraud Pentagon for Detecting Financial Statement Fraud," *Journal of Economics, Business, and Accountancy Ventura*, vol. 22, no. 3, pp. 319-332, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ahmed Hassan, and Ali H. Mhmood, "Optimizing Network Performance, Automation, and Intelligent Decision-Making through Real-Time Big Data Analytics," *International Journal of Responsible Artificial Intelligence*, vol. 11, no. 8, 2021. [Google Scholar] [Publisher Link]

[17] Waleed Hilal, S. Andrew Gadsden, and John Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," *Expert Systems with Applications*, vol. 193, pp. 1-34, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Anayo Chukwu Ikegwu et al., "Big Data Analytics for Data-driven Industry: A Review of Data Sources, Tools, Challenges, Solutions, and Research Directions," *Cluster Computing*, vol. 25, no. 5, pp. 3343-3387, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Soni Agus Irwandi et al., "Detection Fraudulent Financial Statement: Beneish M-score Model," *WSEAS Transactions on Business and Economics*, vol. 16, pp. 271-281, 2019. [Google Scholar]

[20] Mohd Javaid et al., "A Review of Blockchain Technology Applications for Financial Services," *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, vol. 2, no. 3, pp. 1-18, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] Hari Prasad Josyula, "Fraud Detection in Fintech Leveraging Machine Learning and Behavioral Analytics," 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] Pradeep Kumar, and H. Howie Huang, "Graphone: A Data Store for Real-time Analytics on Evolving Graphs," *ACM Transactions on Storage*, vol. 15, no. 4, pp. 1-40, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] Mark E. Lokanan, "Incorporating Machine Learning in Dispute Resolution and Settlement Process for Financial Fraud," *Journal of Computational Social Science*, vol. 6, pp. 515-539, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] Mehdi Mohammadi et al., "Deep Learning for IoT Big Data and Streaming Analytics: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2923-2960, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[25] Manfred Mudelsee, "Trend Analysis of Climate Time Series: A Review of Methods," *Earth-science Reviews*, vol. 190, pp. 310-322, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[26] Aileen Nielsen, *Practical time Series Analysis: Prediction with Statistics and Machine Learning*, O'Reilly Media, 2019. [Google Scholar] [Publisher Link]

[27] Dwi Ratmono, Darsono Darsono, and Nur Cahyonowati, "Financial Statement Fraud Detection with Beneish M-score and Dechow F-score Model: An Empirical Analysis of Fraud Pentagon Theory in Indonesia," *International Journal of Financial Research*, vol. 11, no. 6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[28] Laura Rettig et al., "Online Anomaly Detection Over Big Data Streams," *Applied Data Science*, pp. 289-312, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[29] Roberto Saia, and Salvatore Carta, "Evaluating the Benefits of using Proactive Transformed-domain-based Techniques in Fraud Detection Tasks," *Future Generation Computer Systems*, vol. 93, pp. 18-32, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[30] Varun Shah, "Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats," *Revista Espanola de Documentacion Cientifica*, vol. 15, no. 4, 2021. [Google Scholar] [Publisher Link]

[31] Vanessa Freitas Silva et al., "Time Series Analysis via Network Science: Concepts and Algorithms," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 11, no. 3, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[32] Naomi Clara Situngkir, and Dedik Nur Triyanto, "Detecting Fraudulent Financial Reporting using Fraud Score Model and Fraud Pentagon Theory: Empirical Study of Companies Listed in the LQ 45 Index," *The Indonesian Journal of Accounting Research*, vol. 23, no. 3, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[33] Anuruddha Thennakoon et al., "Real-time Credit Card Fraud Detection Using Machine Learning," *2019 9th International Conference on Cloud Computing, Data Science & Engineering*, Noida, India, pp. 488-493, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[34] Konstantinos Vassakis, Emmanuel Petrakis, and Ioannis Kopanakis, "Big Data Analytics: Applications, Prospects and Challenges," *Mobile Big Data: A Roadmap from Models to Technologies*, pp. 3-20, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[35] Ben Zhang et al., "Awstream: Adaptive Wide-area Streaming Analytics," *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, Budapest Hungary, pp. 236-252, 2018. [CrossRef] [Google Scholar] [Publisher Link]