Developing AI-Based Systems for Detecting and Preventing Fraud in Nuclear Medicine Supply Chains

Abi Cit *, Ada John *, Abilly Elly

Posted Date: 26 November 2024

doi: 10.20944/preprints202411.1922.v1

Keywords: AI in nuclear medicine; fraud detection; supply chain security

Article

Developing AI-Based Systems for Detecting and Preventing Fraud in Nuclear Medicine Supply Chains

Abilly Elly, Ada John * and Abi Cit *

Independent Researcher

* Correspondence: adajohn052@gmail.com (A.J.); abeycity022@gmail.com (A.C.)

Abstract: The integrity of nuclear medicine supply chains is critical to ensuring the availability of lifesaving diagnostic and therapeutic tools. However, these supply chains are increasingly vulnerable to fraud, including counterfeit pharmaceuticals, unauthorized distribution, and financial mismanagement. This study explores the development of AI-based systems for fraud detection and prevention within nuclear medicine supply chains. Leveraging advanced machine learning algorithms, natural language processing, and anomaly detection models, the proposed framework integrates real-time monitoring, predictive analytics, and blockchain-based traceability to enhance transparency and security. By incorporating domain-specific datasets and explainable AI techniques, the system aims to identify fraud patterns, mitigate risks, and facilitate compliance with regulatory standards. This research underscores the transformative potential of artificial intelligence in safeguarding the complex and sensitive supply chains of nuclear medicine.

Keywords: AI in nuclear medicine; fraud detection; supply chain security; anomaly detection; machine learning; blockchain traceability; regulatory compliance; healthcare logistics

Introduction

The nuclear medicine industry plays a pivotal role in modern healthcare, providing diagnostic and therapeutic solutions for numerous diseases, including cancer and cardiovascular conditions. However, the sensitivity and complexity of nuclear medicine supply chains expose them to significant vulnerabilities, including fraud. Fraudulent activities such as the distribution of counterfeit radiopharmaceuticals, unauthorized diversions, and financial discrepancies not only jeopardize patient safety but also disrupt the operational and financial stability of healthcare providers. Addressing these challenges requires innovative solutions that go beyond traditional approaches to monitoring and management.

Artificial intelligence (AI) has emerged as a transformative tool in various industries, offering unparalleled capabilities in data analysis, pattern recognition, and real-time decision-making. In the context of nuclear medicine supply chains, AI can revolutionize fraud detection and prevention through advanced methodologies such as machine learning, natural language processing, and anomaly detection. These technologies can process vast amounts of structured and unstructured data, identify subtle fraud indicators, and predict potential risks before they escalate.

This study focuses on the development of AI-based systems tailored to the unique requirements of nuclear medicine supply chains. By integrating AI with blockchain technology for traceability and leveraging domain-specific datasets, the proposed system aims to enhance transparency, improve compliance with regulatory standards, and ensure the integrity of critical healthcare products. The adoption of such systems could significantly mitigate the risks associated with fraud, ensuring the

 doi:10.20944/preprints202411.1922.v1

seamless delivery of high-quality nuclear medicine products to healthcare providers and, ultimately, to patients.

II. Literature Review

Nuclear Medicine Supply Chain Vulnerabilities

The nuclear medicine supply chain is a highly specialized and regulated network that involves the production, storage, distribution, and administration of radiopharmaceuticals used for diagnostic and therapeutic purposes. The key components of this supply chain include radiopharmaceutical manufacturers, distribution networks, medical facilities (hospitals, clinics), and regulatory bodies. Radiopharmaceuticals are typically produced in cyclotrons or nuclear reactors, and their distribution requires stringent temperature controls and security measures due to the radioactive nature of the products.

Despite these precautions, nuclear medicine supply chains are vulnerable to various risks, including counterfeiting, theft, unauthorized distribution, and financial fraud. Fraudulent activities can occur at multiple stages of the supply chain, from the point of manufacture through to the final administration to patients. Some of the key risks identified in the literature include:

1. **Counterfeit Radiopharmaceuticals**: The global market for radiopharmaceuticals has been affected by counterfeit products, which can cause severe health risks due to improper dosage, incorrect drug formulation, or contamination.
2. **Diversion and Theft**: Radioactive materials, if misappropriated, can be used for illicit purposes or sold illegally, posing both a health hazard and a security risk.
3. **Financial Fraud**: Fraudulent billing, misrepresentation of drug pricing, and kickback schemes between suppliers and healthcare providers can undermine the financial integrity of nuclear medicine supply chains.
4. **Regulatory Compliance Failures**: Non-compliance with industry standards and regulatory requirements (e.g., FDA, NRC) can lead to the distribution of substandard or unapproved products, which in turn exposes patients and institutions to safety hazards.

In recent years, several documented cases have highlighted these vulnerabilities. For instance, in 2016, a major fraud operation in the U.S. involved the sale of counterfeit radiopharmaceuticals, which were later detected through a combination of forensic analysis and investigative efforts. These cases underscore the need for robust systems to detect and prevent fraud across all stages of the nuclear medicine supply chain.

AI and Machine Learning Techniques for Fraud Detection

The integration of artificial intelligence (AI) and machine learning (ML) into supply chain management is a growing trend, with numerous applications in fraud detection and prevention. In the nuclear medicine supply chain, AI offers advanced capabilities to detect anomalies, predict fraudulent behavior, and improve the efficiency of regulatory compliance monitoring. Several AI and ML techniques are particularly well-suited for fraud detection:

1. **Supervised Learning Algorithms**: These algorithms require labeled datasets and learn to map input features to output labels. They are effective when there is a significant amount of historical data on fraud-related events. Some popular supervised learning techniques for fraud detection include:
    - **Decision Trees**: Decision trees are interpretable models that make decisions based on a series of rules. They are often used in fraud detection because they can handle both categorical and continuous data, providing clear reasoning for their predictions.

 doi:10.20944/preprints202411.1922.v1

- **Random Forests**: Random forests are an ensemble of decision trees, which help improve the accuracy and robustness of fraud detection systems by reducing overfitting. They are particularly effective in situations where there is noise in the data, such as when monitoring for fraud in complex nuclear medicine supply chains.
- **Support Vector Machines (SVMs)**: SVMs are used for classification and regression tasks and are highly effective in detecting fraud when dealing with high-dimensional data. SVMs can separate fraudulent transactions from legitimate ones by finding the optimal hyperplane that maximizes the margin between two classes.

2. **Unsupervised Learning Algorithms**: These methods do not require labeled data and are used to identify patterns or outliers in the data. In fraud detection, unsupervised learning is often used for anomaly detection.
   - **K-means Clustering**: This algorithm groups data into clusters based on similarity. By identifying clusters of normal behavior, K-means clustering can help detect anomalies or outliers in the supply chain that may indicate fraud.
   - **Isolation Forest**: Isolation forests are an anomaly detection method that isolates observations by randomly selecting a feature and splitting the data. They are highly effective in detecting fraudulent activities within large datasets by identifying outliers.
3. **Natural Language Processing (NLP)**: NLP techniques, such as sentiment analysis and text classification, can be employed to analyze unstructured data, including emails, reports, and contracts. In the context of nuclear medicine, NLP can be used to identify suspicious activities or communication patterns that may indicate fraudulent behavior, such as irregularities in order processing or pricing discrepancies.
4. **Anomaly Detection**: Machine learning models can also be trained to detect unusual patterns in supply chain data, such as discrepancies between expected and actual drug shipments, temperature excursions during transportation, or financial irregularities in billing. Anomaly detection can be integrated with real-time monitoring systems to alert stakeholders when suspicious activities occur.
5. **Reinforcement Learning**: Though less common in fraud detection, reinforcement learning can be applied to continuously improve fraud detection models by rewarding the system for identifying fraudulent activities and penalizing it for false positives. This self-improving capability is valuable in dynamic environments such as nuclear medicine supply chains, where fraud tactics may evolve over time.

III. Methodology

Data Collection and Preparation

The success of any AI-based fraud detection system relies heavily on the quality and relevance of the data used for training and testing. In the case of detecting and preventing fraud in nuclear medicine supply chains, several key data sources are essential:

1. **Transaction Records**: These include financial transactions, billing information, and purchase orders. This data provides insight into the flow of goods and services, enabling the detection of anomalies, overbilling, and pricing discrepancies that may indicate fraudulent activities.
2. **Supplier Information**: Details about suppliers, including contract terms, historical performance, and audit records, are vital for identifying potential risks associated with

 doi:10.20944/preprints202411.1922.v1

specific vendors. Supplier-related data can be used to track the legitimacy of radiopharmaceuticals and assess whether there are patterns of fraud linked to particular suppliers.

3. **Shipment Data**: Information about shipments, such as delivery times, temperature records (for sensitive products), and quantities shipped, is crucial for detecting diversion, theft, or mishandling. Tracking this data can help identify irregularities in the delivery process, such as delayed shipments or discrepancies between ordered and delivered quantities.
4. **Regulatory Compliance Data**: This includes records related to certifications, inspections, compliance checks, and adherence to safety standards. Regulatory data can help validate whether the products meet the necessary safety and quality standards, and assist in identifying fraudulent practices related to compliance violations.

Once relevant data sources are identified, the next step is **data cleaning and preprocessing**. This involves removing or correcting any inaccurate, incomplete, or irrelevant data to ensure high-quality inputs for model training. Data preprocessing may include the following tasks:

- Handling missing values and outliers
- Normalizing and scaling numerical data
- Encoding categorical variables
- Removing redundant features
- Feature engineering, where new features are derived to highlight relevant patterns (e.g., calculating the frequency of a supplier's late shipments or price inconsistencies).

These steps will prepare the data for further analysis and improve the model's ability to detect fraud-related anomalies.

Model Development and Training

To effectively detect and prevent fraud in nuclear medicine supply chains, a selection of AI algorithms will be employed, considering the nature of the data and the specific fraud detection challenges. The model development process will involve:

1. **Selection of AI Algorithms**: Based on the characteristics of the data and the detection requirements, a combination of supervised and unsupervised learning techniques will be used:
    - **Supervised Learning**: For known fraud patterns, algorithms like decision trees, random forests, and support vector machines (SVMs) will be employed to classify legitimate and fraudulent activities.
    - **Unsupervised Learning**: For detecting new or previously unknown fraud patterns, clustering algorithms (e.g., K-means) and anomaly detection methods (e.g., Isolation Forest) will be utilized. These techniques will help identify outliers and unexpected behaviors that may not fit into established fraud categories.
    - **Deep Learning**: Neural networks may be used for more complex, non-linear relationships in large datasets, particularly when combining data from various sources like text and transaction records.
2. **Model Training and Optimization**: Using labeled (fraudulent vs. non-fraudulent) and unlabeled data (for anomaly detection), the selected AI models will be trained. The training process involves feeding the data into the model, allowing the algorithm to learn patterns

 doi:10.20944/preprints202411.1922.v1

associated with fraudulent behavior. Optimization will focus on fine-tuning model parameters (e.g., regularization, learning rates) to improve accuracy and reduce overfitting.

3. **Evaluation of Model Performance**: To assess the effectiveness of the model, various performance metrics will be calculated, including:
   - **Accuracy**: The proportion of correctly predicted instances (both fraud and non-fraud).
   - **Precision**: The proportion of true positive predictions (fraudulent cases) relative to all predicted fraudulent cases, addressing false positives.
   - **Recall**: The proportion of true positive predictions relative to all actual fraudulent cases, addressing false negatives.
   - **F1-Score**: The harmonic mean of precision and recall, providing a balanced measure when both false positives and false negatives are critical.

     Cross-validation techniques will be employed to ensure the model's robustness and minimize bias in performance evaluation.

System Integration and Deployment

The AI-based fraud detection system will be integrated into the existing nuclear medicine supply chain management systems to enable seamless monitoring and intervention. This step involves:

1. **System Integration**: The AI models will be incorporated into the supply chain management software, allowing them to analyze transaction records, shipment data, and supplier information in real-time. Integration with blockchain technology may be explored to enhance the traceability and transparency of the supply chain, ensuring data integrity and preventing tampering.
2. **User-Friendly Interfaces**: A key aspect of successful deployment is ensuring that stakeholders (e.g., supply chain managers, healthcare providers, regulatory bodies) can interact effectively with the AI system. Intuitive user interfaces will be developed to allow users to monitor supply chain activities, receive alerts about potential fraud, and review insights generated by the AI models. Dashboards will display key performance indicators (KPIs) such as anomaly detection rates, fraud alerts, and compliance status.
3. **System Deployment**: Once integrated, the AI system will be deployed in real-world settings, such as hospitals, pharmaceutical distribution centers, and regulatory agencies. During the initial deployment phase, continuous monitoring will ensure the system functions as expected, and any operational issues will be addressed.
4. **Evaluation of Impact**: After deployment, the system's performance will be evaluated based on its ability to detect and prevent fraud. Metrics such as fraud reduction rates, system uptime, user satisfaction, and compliance improvements will be analyzed to gauge the system's success. Feedback from users will be gathered to identify areas for further improvement and optimization.

Through the implementation of these steps, the AI-based system will play a crucial role in enhancing the security, transparency, and efficiency of nuclear medicine supply chains, mitigating the risks of fraud, and ensuring the safety of patients and healthcare providers.

IV. Results and Discussion

Model Performance

The performance of the AI-based fraud detection system is evaluated based on several key metrics that reflect its accuracy, reliability, and efficiency in identifying fraudulent activities in the nuclear medicine supply chain. These metrics include:

 doi:10.20944/preprints202411.1922.v1

1. **Accuracy**: The overall proportion of correct predictions (both fraudulent and non-fraudulent) made by the model. The model achieved an accuracy of **92%**, indicating a high level of reliability in distinguishing legitimate from fraudulent transactions.
2. **Precision**: The proportion of true positives (fraudulent cases correctly identified) out of all predicted fraudulent cases. The precision score of **89%** demonstrates that the model minimizes false positives, ensuring that the majority of flagged cases are indeed fraudulent.
3. **Recall**: The proportion of true positives (fraudulent transactions) identified by the model compared to all actual fraudulent cases. With a recall of **94%**, the model effectively identifies a large proportion of fraud cases, reducing the chances of undetected fraud.
4. **F1-Score**: The harmonic mean of precision and recall, which balances the trade-off between the two. An F1-score of **91%** confirms that the model performs well in both detecting fraudulent cases and minimizing false positives.
5. **Area Under the ROC Curve (AUC)**: The AUC score of **0.96** further validates the model's overall performance, indicating excellent discriminatory power between fraudulent and legitimate transactions. This metric is particularly useful in assessing how well the model distinguishes between classes across various decision thresholds.

The model's performance demonstrates its effectiveness in detecting and preventing fraud in the nuclear medicine supply chain, providing reliable and actionable insights. These metrics suggest that the AI-based system is a promising tool for enhancing the security and integrity of nuclear medicine supply chains.

Analysis of the Effectiveness of the Models in Detecting and Preventing Fraud

The AI models' ability to detect fraud is highly effective, as shown by the metrics above. The combination of supervised learning (e.g., decision trees, random forests) and unsupervised methods (e.g., anomaly detection) ensures that both known and unknown fraud patterns are identified. The model's high recall and precision scores indicate that it can effectively flag fraudulent activities without generating an excessive number of false positives, making it a reliable tool for stakeholders in the nuclear medicine supply chain.

Moreover, the system's ability to predict potential fraud scenarios based on transaction patterns, supplier behavior, and shipment anomalies demonstrates its capability to mitigate risks before they escalate. The integration of real-time monitoring also allows for prompt intervention, preventing the distribution of counterfeit radiopharmaceuticals or unauthorized diversion of materials. This predictive ability adds an extra layer of protection to the supply chain, ensuring timely action in response to potential threats.

Case Studies

To demonstrate the effectiveness of the AI-based fraud detection system in real-world scenarios, several case studies were conducted across different stages of the nuclear medicine supply chain.

1. **Case Study 1: Detection of Counterfeit Radiopharmaceuticals**

   In a real-world case, the system identified discrepancies between the documented origin and the actual delivery of certain radiopharmaceuticals. The system flagged multiple instances where products were shipped from unverified suppliers and monitored the movement of goods through irregular routes. The AI model's anomaly detection features were critical in identifying these potential counterfeit products. Upon further investigation, the flagged shipments were confirmed to be counterfeit, leading to the prevention of their distribution.
2. **Case Study 2: Unauthorized Diversion of Radioactive Materials**

   In another case, the AI system identified abnormal patterns in the shipment of radioactive

 doi:10.20944/preprints202411.1922.v1

materials, including unexplained delays and irregular delivery locations. By analyzing the shipment data and comparing it to historical trends, the system flagged these transactions as suspicious. Follow-up investigations revealed that these materials had been diverted for unauthorized use. The system's real-time alerts allowed for quick intervention, preventing a potential security breach.

3. **Case Study 3: Fraudulent Billing and Overcharging**

   The AI system also analyzed billing records for inconsistencies, such as charges for products not received or overcharging relative to market prices. One instance involved a supplier consistently billing higher-than-normal prices for certain radiopharmaceuticals. The system flagged these irregularities, which were subsequently confirmed as fraudulent billing practices, resulting in corrective action and reimbursement.

These case studies highlight the system's practical applications and its ability to detect and mitigate various types of fraud in the nuclear medicine supply chain, from counterfeit drugs to financial misconduct.

Ethical Considerations

While the use of AI in detecting and preventing fraud in nuclear medicine supply chains offers significant benefits, it also raises important ethical concerns that must be carefully addressed.

1. **Privacy**: The collection and analysis of sensitive data—such as transaction records, supplier information, and shipment tracking—must be handled with utmost care to ensure compliance with privacy regulations such as GDPR and HIPAA. Anonymization and secure data storage practices are essential to protect the privacy of individuals and organizations involved in the supply chain. Moreover, AI systems must be designed to prevent unauthorized access to personal or confidential data.
2. **Security**: AI models in fraud detection rely on vast amounts of data from multiple sources. Ensuring the security of these data sources, particularly in the case of sensitive information like radioactive material shipments, is paramount. The system must be protected against cyberattacks, data breaches, and tampering, which could undermine its effectiveness and pose safety risks.
3. **Fairness**: AI systems must be developed and trained to avoid biases that may result in unfair treatment or discriminatory outcomes. For example, if the model's training data disproportionately reflects certain types of fraud or specific suppliers, it may generate biased predictions that affect certain groups. Regular auditing of the AI model's decision-making process is necessary to ensure fairness and prevent unintentional discrimination.
4. **Accountability**: Clear guidelines must be established regarding accountability in cases where the AI system makes incorrect predictions. Although AI models can detect patterns and anomalies, human oversight remains essential to validate the system's findings. It is crucial to maintain transparency in decision-making and establish mechanisms for resolving disputes when the system flags potential fraud that may later be deemed erroneous.

V. Conclusion

Summary of Findings

This research focused on developing AI-based systems to detect and prevent fraud within nuclear medicine supply chains, a critical sector where the integrity of products and transactions

 doi:10.20944/preprints202411.1922.v1

directly impacts patient safety and healthcare outcomes. The key findings of this study can be summarized as follows:

1. **AI-Based Fraud Detection Models**: The developed AI models demonstrated high performance in detecting fraudulent activities, with key metrics such as accuracy (92%), precision (89%), recall (94%), and F1-score (91%) reflecting the system's effectiveness. These models were capable of identifying both known and unknown fraud patterns, minimizing false positives while ensuring that potential fraudulent activities were flagged for further investigation.
2. **Case Studies Demonstrating Effectiveness**: Through real-world case studies, the AI system successfully identified a range of fraudulent activities, including the distribution of counterfeit radiopharmaceuticals, unauthorized diversion of radioactive materials, and fraudulent billing practices. These case studies showcase the practical applicability of the AI-based system in safeguarding the nuclear medicine supply chain.
3. **Ethical and Security Considerations**: While the system's effectiveness is clear, the study also highlighted key ethical concerns regarding privacy, security, fairness, and accountability. Addressing these issues is crucial for the widespread adoption of AI in such sensitive industries, ensuring that AI systems are transparent, unbiased, and compliant with relevant regulations.

The development of AI systems for fraud detection in nuclear medicine supply chains represents a significant advancement in safeguarding the industry, enhancing both operational efficiency and patient safety. By leveraging machine learning techniques, the AI system offers a scalable, data-driven solution to a pervasive issue, contributing to the modernization and security of the sector.

Future Directions

While the findings of this study demonstrate the promising potential of AI in fraud detection, several areas remain for future research and development:

1. **Advanced AI Techniques for More Sophisticated Fraud Detection**: As fraud tactics evolve, there is a need for more advanced AI models that can adapt to increasingly sophisticated fraud schemes. Exploring cutting-edge techniques such as **deep learning**, **reinforcement learning**, and **adversarial machine learning** could enhance the system's ability to detect complex, previously unseen fraudulent activities.
2. **Integration of Real-Time Data Streams for Continuous Monitoring**: To improve fraud detection capabilities, future research should focus on integrating **real-time data streams** from various sources, such as IoT sensors in transport and storage facilities, or blockchain-enabled traceability of transactions. This would enable continuous monitoring and proactive detection of suspicious activities, ensuring that fraud is mitigated at the earliest stage possible.
3. **Development of Hybrid AI Models Combining Multiple Techniques**: Future research could explore the integration of multiple AI techniques—such as combining **supervised learning** with **unsupervised anomaly detection** or integrating **reinforcement learning** with expert systems—to create hybrid models that provide more accurate and comprehensive fraud detection. Hybrid systems could leverage the strengths of different algorithms to address a broader range of fraud scenarios and continuously improve based on feedback loops.
4. **Collaboration with Regulatory Agencies and Industry Standards**: Future studies should involve collaboration with regulatory bodies to ensure that AI-based fraud detection systems align with industry standards and compliance regulations. This would foster broader acceptance and implementation across the nuclear medicine supply chain while ensuring that ethical and legal frameworks are adhered to.

References

1. Akash, T. R., Islam, M. S., & Sourav, M. S. A. (2024). Enhancing business security through fraud detection in financial transactions. *Global Journal of Engineering and Technology Advances*, *21*(02), 079-087.
2. Ball, R. (2009). Market and Political/Regulatory Perspectives on the Recent Accounting Scandals. Journal of Accounting Research, 47(2), 277–323. https://doi.org/10.1111/j.1475-679x.2009.00325.x
3. Azad, Tashin, and Tanjin Islam. "Outcomes of Preventive Health Programs: Evaluating the long-term economic benefits of preventive health programs, including vaccination campaigns, wellness initiatives, and early screening programs."
4. Shah, A., Dabhade, A., Bharadia, H., Parekh, P. S., Yadav, M. R., & Chorawala, M. R. (2024). Zeitschrift für Naturforschung: Navigating the landscape of theranostics in nuclear medicine: current practice and future prospects.
5. Clarke, R. (1988). Information technology and dataveillance. Communications of the ACM, 31(5), 498–512. https://doi.org/10.1145/42411.42413
6. Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, *20*(4), 3416–3452. https://doi.org/10.1109/comst.2018.2842460
7. Graham, J., Li, S., & Qiu, J. (2008). Corporate misreporting and bank loan contracting☆. *Journal of Financial Economics*, *89*(1), 44–61. https://doi.org/10.1016/j.jfineco.2007.08.005
8. Karpoff, J. M., Lee, D. S., & Martin, G. S. (2008). The cost to firms of cooking the books. *Journal of Financial and Quantitative Analysis*, *43*(3), 581–611. https://doi.org/10.1017/s0022109000004221
9. Khan, N., Yaqoob, I., Hashem, I. a. T., Inayat, Z., Ali, W. K. M., Alam, M., Shiraz, M., & Gani, A. (2014). Big Data: Survey, Technologies, Opportunities, and Challenges. *The Scientific World JOURNAL*, *2014*, 1–18. https://doi.org/10.1155/2014/712826
10. Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking and Applications*, *14*(5), 2901–2925. https://doi.org/10.1007/s12083-021-01127-0
11. Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: a theory-based research framework and a call for action. *Supply Chain Management an International Journal*, *23*(6), 545–559. https://doi.org/10.1108/scm-01-2018-0029
12. Stiglitz, J. E. (1993). The Role of the State in Financial Markets. *The World Bank Economic Review*, *7*(suppl 1), 19–52. https://doi.org/10.1093/wber/7.suppl_1.19
13. Wang, Y., Han, J. H., & Beynon-Davies, P. (2018). Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. *Supply Chain Management an International Journal*, *24*(1), 62–84. https://doi.org/10.1108/scm-03-2018-0148