Meta-Synthesis of Organisational Barriers to Decision Tree Data Analytics Adoption in Payment-Fraud Operations

PANKAJKUMAR TEJRAJ JAIN[1], ASHOK GHIMIRE[2], RESHMA LESLIE[3], SANDEEP SHRESTHA[4]
[1,2,3,4] *Department of Business Administration, Westcliff University, Irvine*

Abstract: Increased incidences of payment fraud in the financial sector thus saw the increased use of advanced data analytic tools to detect and prevent fraudulent transactions. Among these tools, Decision Tree models are highly valued for their interpretability, simplicity in implementation, and their ability to classify and predict fraudulent behavior. However, from a practical point of view, and despite the technical prowess of Decision Tree analytics, adoption of these in payment-fraud operations remains scant. This study presents a meta-synthesis of existing qualitative studies to investigate the organizational barriers that hinder the adoption of Decision Tree data analytics in fraud detection processes. It synthesizes findings from diverse industry and academic sources and reveals the principal challenges these organizations face in integrating these technologies into their fraud operations. The meta-synthesis brings out some of the main barriers to adoption, among which are: cultural resistance against machine learning tools; organizational resistance against embracing algorithmic decision-making; and distrust towards any automated system. Meanwhile, there are huge skill and knowledge deficits, since many organizations have a hard time locating personnel sufficiently trained in both implementing and interpreting Decision Tree models. Other data-related issues emerged as key challenges that hindered the construction of good models: data silos fragmented within organizations and poor data quality. Moreover, legacy infrastructure and expensive integration thwarted were substantial hindrances in organizations with legacy systems. Strategic misalignment, where fraud analytics goals are not sufficiently tied to larger business objectives, inhibits the more successful adoption of analytics. It supports the view that in overcoming these barriers, organizations should nurture a data-driven culture, encourage cross-functional collaboration, and commit resources to technical infrastructure and talent development. In addition, these insights fit well within technology adoption frameworks, describing how the interference of organizational, culture, and strategic issues may affect uptake of Decision Tree analytics. Providing actionable recommendations, this study should provide fertile ground for institutions, fintech entities, and payment processors willing to reach further in fraud detection. The research further calls for additional work, especially longitudinal and sector-specific, to lay the adoption issues and opportunities within fraud prevention in a broader light throughout its metamorphosis.

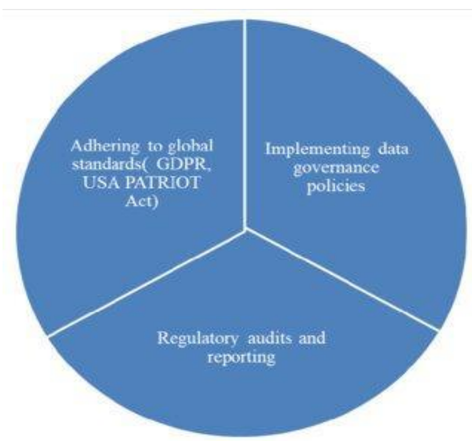
Indexed Terms- Decision Tree analytics, payment fraud detection, organizational barriers, technology adoption, machine learning, fraud operations, meta-synthesis, data analytics, organizational culture, infrastructure challenges, strategic alignment.

I.

I. INTRODUCTION

Because digital payment systems are evolving rapidly, both consumers and companies now enjoy greater ease and speed. Still, the new way of paying has resulted in more cases of fraud which could threaten the safety and trust needed for handling financial transactions. To deal with these new threats, businesses now depend on advanced data analytics when fighting against fraud. Many experts in fraud detection use decision tree methods, since they can efficiently and clearly classify and forecast fraud. As fraud detection systems rely on rules, algorithms with a logical structure are especially appealing for use in financial fraud prevention.

Even though Decision Tree algorithms offer useful abilities, organizations have not been quick to apply them in the fight against payment fraud as technology has progressed. There are many cases in which financial organizations, fintech firms and payment processors lack advanced methods for guarding against fraud. It is not only a problem of having suitable technology; it is commonly caused by other, more involved features of the company. Examples are resistance to new developments, a shortage of necessary workers, concerns about using unfamiliar systems and doubt about the benefits from the change. Therefore, identifying the obstacles related to how organizations use Decision Tree-based analytics is key to making sure innovations happen in practice.



This research began because there is a need to identify the obstacles that prevent Decision Tree methods from being used effectively against fraud. While technical information about algorithms and their performance is easy to find, information about the human, structural and institutional sides of using them in practice is missing. With a detailed look at these barriers, this research tries to summarize the main challenges faced by organizations, so that others can make smarter and more informed moves in the industry.

Since it explores organizational challenges only, the study completely ignores technical constraints and problems with algorithms that have been discussed in other places. The evaluation of these methods will occur in contexts involving financial institutions, fintech companies and payments processors because the risks of fraud detection are very high and strong analytics can matter greatly. Additionally, the research admits that its results cannot be taken to other sectors or categories of data analytics for certain. Yet, investigating organizational factors helps the study highlight an important aspect of undertaking data analytics in fraud control efforts.

II. LITERATURE REVIEW

The field of machine learning has seen Decision Tree analytics as an important tool for classification and prediction problems. CART, C4.5 and CHAID are examples of these models that separate data into sections according to rules decided from the input variables. A reason why Decision Tree models are attractive in fraud detection is that they are easily understandable. Compared to many lesser-known algorithms, Decision Trees make their reasoning clear so that human analysts and stakeholders can easily check and confirm them. The capability to manage all kinds of data, plus their stability with gaps in numbers and unusual correlations, makes them well-adapted to financial fraud monitoring.

Decision Trees have recently become a popular method for detecting payment fraud by both experts and practitioners working in the industry. These algorithms are now used in both banking and fintech companies to find and prevent fraud. A number of research papers and real-life experiences prove that Decision Trees are highly effective in finding unusual activity, marking unpredictable actions and boosting the initial accuracy of fraud detection. Even used by themselves, trees are useful because they are fast, scalable and easy to understand and their usefulness is further increased if used as part of Random Forests or Gradient Boosted Trees. Adding these models to transactional monitoring systems after proper training has been found to reduce the number of false positives and help fraud detection.

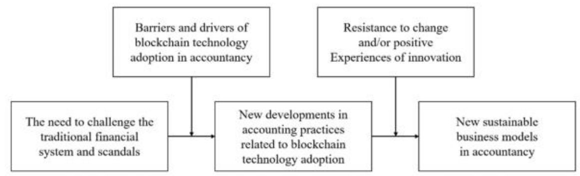
Still, Decision Tree analytics in the payment-fraud field is not widely adopted by most companies. Many studies point to several factors other than technology that make it hard to add such tools to existing processes. These theoretical frameworks, including the Technology-Organization-Environment (TOE) framework, the Technology Acceptance Model (TAM) and the Diffusion of Innovations (DOI) theory, give us a clear way to examine the influences on technology adoption. They focus on how preparations within organizations, help from managers, opinions about innovation in the work culture and expected advantages from using the technology shape whether or not adoption will take place. Despite recognizing the potential of Decision Trees, a financial institution's unwillingness to change, worries about data management, a shortage of trained experts or a mismatch with current decision-making may really limit their use.

Also, the use of advanced analytics and AI commonly needs more than just getting new software or hiring computer experts. It requires companies to think differently, upgrade their infrastructure and be ready for long-term improvement. Operations-bound or cautious firms are often challenged to approach these requirements in a way that fits with what they can do. That's why in finance and other regulated fields, where adherence, verification and security are key, having this information is especially valuable. According to the literature, if these issues are ignored, perhaps the most powerful analytical tools cannot fulfill their purpose.

The repository of existing research points toward a dual reality: while Decision Tree analytics hold the prospect of enhancing payment-fraud detection substantially, the successful adoption of such systems would depend not only on the technically sound method but an appreciative knowledge of the organizational reality as well. This literature review thus prepares the background for an exploration into these organizational challenges, setting the context in which adoption decisions are made and stressing the urgency of bridging the gap between analytical innovation and institutional readiness.

III. RESEARCH METHODOLOGY

In order to identify and analyze the organizational issues preventing the use of Decision Tree analytics in payment-fraud tasks, the study takes a qualitative meta-synthesis approach. Meta-synthesis is not like quantitative meta-analysis which sums up raw information to draw general results. Instead, it involves studying and putting together the findings of existing qualitative studies. It works well for things like organizational behavior, how institutions make choices and resisting technological changes, all of which depend more on context and meaning than on statistics. By means of meta-synthesis, we learn how organizations can better cope with the obstacles of making use of advanced analysis methods. Because the purpose of this research is to understand organizations rather than algorithmic results, a qualitative approach gives more interpretive space and flexibility.



The decision about the papers to be considered in the meta-synthesis was made so that it would include only ones that were important, believable and comprehensive. Searches were made on Scopus, Web of Science, IEEE Xplore, ScienceDirect and Google Scholar. We looked for articles by using carefully selected search terms and Boolean operations such as "Decision Tree analytics," "fraud detection," "organizational challenges," "using advances in technology," "financial institutions," and "AI implementation." Only studies that discussed the organizational or managerial approaches to using data analytics or AI in financial or payment systems and provided qualitative information or a mix of methods, were included. Studies that concentrated only on how an algorithm worked and did not incorporate an organizational element or were not about finance or fraud were not included. Priority was set for publications from journal articles, conference proceedings and case studies, all published during the last ten to fifteen years.

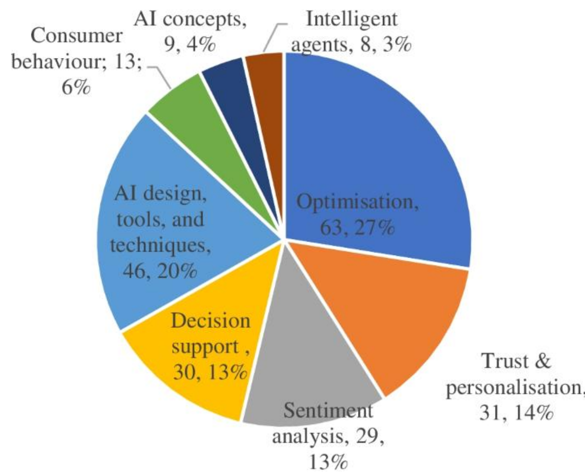
Data extraction and analysis were done on a group of suitable studies using reliable qualitative research approaches. Recurring topics and trends were found through carrying out thematic coding for organizational barriers. To do this, researchers kept reading, annotating and coding the documents to find main themes that would let them compare the different studies. The model of synthesis selected for this study is Noblit and Hare's meta-ethnography. With this method, key points from different sources are linked together in a new framework, resulting in a wider understanding than is typically seen in any one study. Using meta-ethnography, experts build "third-order interpretations" by looking at how previous research relates to one another, rather than by conducting new data surveys.

This study aims to create an interpretive summary of what the current literature has revealed about organizational problems with adopting Decision Tree analytics for fraud detection. By closely reviewing many types of qualitative findings, the research aims to find similarities, contrasting opinions and unexpected ideas useful for both research and practical approaches to building casting companies' readiness in the face of new analytical tools.

IV. FINDINGS AND THEMATIC SYNTHESIS

This effort showed that several themes are related and explain the main barriers to using Decision Tree analytics to detect payment fraud in organizations. They reveal that, even though technology is usually effective for the task, it often faces difficulties fitting into the organization's existing framework.

Many of the writings on leadership point out how organizations and cultures can get in the way of leaders. It is common for institutions to distrust machine learning in important fields, since people, not machines, have usually been in charge of fraud detection. Because humans can easily understand Decision Tree models, many fraud analysts and managers still prefer the clearer rules seen in other types of AI. It gets worse when organizations with established processes and a traditionally conservative work environment resist change. Moving from traditions and manual methods to decision-making guided by evidence and software algorithms involves much more than technology—many organizations find it difficult or unappealing.



On top of all this, many organizations are also missing key skills and knowledge. Decision Tree analytics should be used with experts in building and adjusting models as well as operational personnel who understand the outcomes and know how to turn them into real decisions. Not many organizations have all the appropriate skills needed to support the full use of analytics. So, they often depend a lot on consultants or vendors which may complicate the costs, the way data is managed and bringing together various systems. Outsourcing expertise can be useful in the short run, but it tends to slow down the growth of your own team and hurt the long-term success of your analytics efforts.

Data problems turned out to be a major topic in the consolidated findings. To work well, Decision Tree models require data that is up to date, accurate and thorough. It is worrying to see that many businesses operate in siloed data spaces, where details are kept separately or in formats that don't match. Bad data, gaps in records and different labeling methods often decrease the effectiveness of fraud detection models during training and in use. Using financial data that requires protection leads to key concerns regarding people's privacy, the safety of their data and fulfilling regulatory rules. Dealing with these limitations can make data governance more difficult and around the world, strongly enforced data protection laws often lead to a lengthy time to adopt analytics.

Additional limits come from infrastructure not being capable enough and the expense of using Decision Tree methods. Many old established financial institutions use IT infrastructure that is too old to support the modern analytics tools they require. Setting up Decision Tree systems in these fields normally means spending a lot on new equipment, programs and updates—spending that is hard to justify unless the results are quick. After setting up a machine learning model, additional expenses to update and monitor it are a problem for some organizations.

Finally, research findings showed that misalignment between strategy and action is a key problem. In many instances, analytics groups are not tied to major business goals which can limit their ability to maintain support from top executives. When fraud detection does not support the main goals of the business—such as satisfying clients, running efficiently or meeting the rules—it often does not get the approval of senior leadership. Those in leadership may think of analytics as a peripheral issue instead of seeing its value, so they don't focus on the reforms necessary to put these tools to daily use.

By looking at all these themes together, we can fully understand the different roadblocks to bringing Decision Tree analytics into practice when detecting payment-fraud. The clever insights offered by advanced analytics are clear, yet getting them to work effectively involves overcoming complicated issues in culture, technology and strategy.

V. DISCUSSION

The study findings support and at times expand on the literature on using technology in financial institutions. Many of the studies done today put emphasis on achieving better technical outcomes, greater model accuracy and more complex algorithms, while paying less attention to the work environment in which the technology will be used. By using qualitative methods and grouping data into themes, the study confirms that culture, infrastructure and strategy matter at least as much or more, than training and experience in the adoption of new analytical tools. As expected by earlier studies, my data shows that the most important challenges are resistance to changes, employees lacking the necessary skills and not having the same goals as expected. It is noteworthy, however, that this research illustrates in detail how these problems appear when implementing Decision Tree analytics for fraud detection, a topic often neglected in the analytics literature.

The difference from past studies here is that it looks closely at Decision Tree models, rather than considering general AI or machine learning. Applying Decision Trees did not prevent the challenges associated with inertia and a disconnect in planning. Many technology-centered studies assume that the fact something is simple and understandable always makes it easier to use, but this is not always correct. In fact, things are not that simple; the organization's environment should be able to accept and work with these tools, no matter how impressive or suitable the theories behind them seem.

For anyone overseeing fraud duties in financial institutions, fintech firms or payment processors, the results of this study have meaning. This tells us that making sure analytics technologies align with an organization's culture and that its leaders are fully engaged is as important as ensuring the models work well. Anyone preventing fraud should do more than just acquire sophisticated tools; they should also focus on developing skills, working with different teams and matching their analytics efforts with overall company objectives. You should treat training your employees, managing activities during the change process, removing data barriers and upgrading the system as important to success as choosing the correct algorithm. At the same time, executive teams must understand that embracing analytics is an ongoing strategy that must start at the top to take off and become useful.

The article introduces domain-specific findings from fraud analytics which enhance the current frameworks used to study technology adoption. TAM, TOE and the Diffusion of Innovations are useful ways to understand how things get adopted, but they work best when adapted to the specific environment. The study demonstrates that, despite positive conditions, specific challenges such as not trusting algorithms, concerns over how companies use data and teams in different places can still greatly hinder progress in fraud detection efforts. Based on these results, technology adoption theory should be improved with modifiers that address the unique issues businesses face in strict and risk-averse sectors such as finance.

The holistic discussion highlights the point that Decision Tree analytics, in terms of fraud detection, is not just a technical decision but rather a complex organizational one. Interventions are needed across multiple layers of the organization to address the barriers described in this study, thereby closing the gap between analytical ability and operational execution.

RECOMMENDATIONS

Based on the findings and thematic synthesis, it becomes clear that Decision Tree analytics' successful adoption for payment-fraud detection brings with it more than mere technical readiness. Organizations need to deliberately engage in other complementary steps to overcome the structural and cultural barriers unearthed in this study. At the heart of these efforts should be meaningful organizational change that supports data-driven decision-making, starting with the emergence of a culture that valued and trusted analytical insights. In the daily operations of their organizations, however, leaders should promote the use of data and analytics by encouraging openness toward the tools of machine learning, alleviating any fears that these tools might somehow diminish human expertise, and instead creating an environment embracing analytics as a great strategic asset. The decision to open a dialogue and resistance to analytics must be fought against since only then will Decision Trees in fraud detection workflows be brought to life.

In support of the cultural change, organizations should engage in training and capacity-building programs as well. Training internal staff is vital: data scientists need it, but so do fraud analysts, compliance officers, and decision-makers who use analytical tools. These stakeholders should learn the practical aspects of Decision Tree models-how the models work, the interpretation of model outputs, and how to apply model-enhanced insights to anti-fraud countermeasures. Promoting cooperation among IT, analytics, and fraud operations teams may go on to further efforts to enhance knowledge sharing and ensure alignment between analytics initiatives and the realities on the ground. Structure training programs, mentor, and practice model simulations -- confidence and skills must be cultivated to power fraud operations with analytics. Alongside cultural and human capital investments, an organization must also consider the technical foundation it needs to make scalable analytics adoption a reality. Legacy infrastructure is too often a roadblock, especially for institutions that have been formed through mergers or where there is no centralized data architecture. To get past this, organizations should be looking for modular and scalable infrastructure solutions that support Decision Tree analytics and other machine learning tools and do not require top-to-bottom system overhauls. Cloud-based platforms and data lakes are amongst many viable options to choose from. Investing in adaptable systems also means that your analytics capabilities will stand the test of time and do not get left behind when new fraud patterns and regulatory requirements come around.

In sustaining remuneration, technical diversifications are necessary. With the sensitivity of financial data on the utmost side, regulators are scrutinizing data much more, and hence the data management frameworks developed by organizations must be of high sturdiness, with procedures being defined for data access, storage, quality assurance, and model audit. An ethical perspective should be integrated into the entire analytics life cycle, regarding customer privacy, algorithm transparency, and bias reduction. Governance mechanisms should be in place not only to guard against potential abuse of governance-related activities but also to build trust among stakeholders so that they believe in the models they see as dependable and fair. As reviewed periodically, these frameworks must remain open and flexible, adjusting to any changes in the applicable laws and morals.

These recommendations describe the magnum opus of enabling organizational conditions for efficiently embedding Decision Tree analytics into payment-fraud detection. When cultural, human, technical, and governance elements come into alignment, institutions become capable of bringing analytical possibilities into operational realities and increasing their ability to detect and prevent fraudulent activities within an increasingly complex financial environment.

CONCLUSION

By analyzing the organizational barriers to Decision Tree analytics in payment-fraud detection, this study has presented a thorough overview. The key insights at hand emphasize that Decision Trees possess huge potential for bolstering fraud detection capabilities; yet multiple organizational obstacles usually stand between the industries and the actual operationalization of this approach. These inhibiting factors include culture-based resistances, skill and knowledge shortages, issues related to data, infrastructure drawbacks, and finally, strategic mismatch or misalignment. Thus, notwithstanding all enhancements and robust interpretability offered by Decision Tree models from a technical viewpoint, these barriers illustrate how the deployment of any extended set of analytical skills encompasses much more than the bare technical preparedness. Hence, organizations would do well to tackle ingrained cultural perspectives, work toward workforce development improvements, and upgrade their infrastructure so as to take full advantage of data-driven methods in fraud prevention.

The importance of removing organizational barriers cannot be overstated. Although Decision Tree model capabilities have been highly touted, their practical implementation in fraud detection environments is too often hindered by factors that should, in many cases, be easily controlled by the very organization that they hinder.By dint of setting in place a data culture and investing in training, infrastructure improvement, and governance framework design, organizations shed their limits toward unlocking fraud analytics. Without addressing such challenges, the fraud detection system, no matter how talented, could continue to remain mostly unused, ultimately leading to payment system vulnerabilities.

Going forward, there are several directions for future research that could further build on the present study. For instance, longitudinal studies can ascertain how organizations evolve their adoption of Decision Tree analytics over time, thereby presenting a rather dynamic view of the process. Studies geared toward sector-specific barriers would also prove to be helpful because different sectors are prone to different regulatory, cultural, and operational constraints. Additionally, studies to analyze how Decision Tree models perform in actual fraud detection in a range of institutional settings would provide greater insight into the efficacy of such models as well as the organizational change needed for successful implementation of them.

This study points out that using Decision Tree analytics as a complete system is crucial for managing payment-fraud risks. Merely getting new tools is not enough; companies should focus on overcoming barriers facing culture, organization and technology. With financial fraud constantly changing, the need to overcome these issues will become more significant, pointing to how ready an organization is to use new technologies.

REFERENCES

[1] Mostafapoor, H., Keramati, M., Mehrinejad, S., & Minouei, M. (2024). Application of Meta-Synthesis Technique in Bank Profitability Model Considering the Role of Modern Banking Technologies. Management Strategies and Engineering Sciences, 6(2), 15-24.

[2] Shakibaei Bonakdeh, E., Sohal, A., Rajabkhah, K., Prajogo, D., Melder, A., Nguyen, D. Q., ... & Tong, E. (2024). Influential factors in the adoption of clinical decision support systems in hospital settings: a systematic review and meta-synthesis of qualitative studies. Industrial Management & Data Systems, 124(4), 1463-1500.

[3] Adabi, M. Application of Meta-Synthesis Technique in Human Resource Educational Management Based on Artificial Intelligence.

[4] Pigola, A., & Da Costa, P. R. (2023). Dynamic capabilities in cybersecurity intelligence: A meta-synthesis to enhance protection against cyber threats. Communications of the Association for Information Systems, 53(1), 1099-1135.

[5] Bello, O. A., Ogundipe, A., Mohammed, D., Adebola, F., & Alonge, O. A. (2023). AI-Driven Approaches for real-time fraud detection in US financial transactions: challenges and opportunities. European Journal of Computer Science and Information Technology, 11(6), 84-102.

[6] Ejiofor, O. E. (2023). A comprehensive framework for strengthening USA financial cybersecurity: integrating machine learning and

AI in fraud detection systems. European Journal of Computer Science and Information Technology, 11(6), 62-83.

[7] Oladeinde, M., Hassan, A. O., Farayola, O. A., Akindote, O. J., & Adegbite, A. O. (2023). Review of it innovations, data analytics, and governance in nigerian enterprises. Computer Science & IT Research Journal, 4(3), 300-326.

[8] Sumankuuro, J., Crockett, J., & Wang, S. (2018). Sociocultural barriers to maternity services delivery: a qualitative meta-synthesis of the literature. Public health, 157, 77-85.

[9] Vasudevan, A., & Ford, E. (2022). Motivational factors and barriers towards initiating and maintaining strength training in women: a systematic review and meta-synthesis. Prevention Science, 23(4), 674-695.

[10] Li, X., Yang, C., Møller, C., & Lee, J. (2024). Data Issues in Industrial AI System: A Meta-Review and Research Strategy. arXiv preprint arXiv:2406.15784.

[11] Nguyen, Q. T., Tran, T. N., Heuchenne, C., & Tran, K. P. (2022). Decision support systems for anomaly detection with the applications in smart manufacturing: a survey and perspective. In Machine Learning and Probabilistic Graphical Models for Decision Support Systems (pp. 34-61). CRC Press.

[12] Xu, B., & Wang, S. (2024). Examining windows file system irp operations with machine learning for ransomware detection.

[13] Fazel, E., Nezhad, M. Z., Rezazadeh, J., Moradi, M., & Ayoade, J. (2024). IoT convergence with machine learning & blockchain: A review. Internet of Things, 101187.

[14] Tragouda, M., Doumpos, M., & Zopounidis, C. (2024). Identification of fraudulent financial statements through a multi-label classification approach. Intelligent Systems in Accounting, Finance and Management, 31(2), e1564.

[15] Ejaz, U., & Gimah, M. (2024). AI in Subscription-Based Services for Churn Detection.

[16] Merhej, J., Harb, H., Abouaissa, A., & Idoumghar, L. (2024). Toward a New Era of Smart and Secure Healthcare Information Exchange Systems: Combining Blockchain and Artificial Intelligence. Applied Sciences, 14(19), 8808.

[17] Rodríguez Cardona, D., Werth, O., Schönborn, S., & Breitner, M. H. (2019). A mixed methods analysis of the adoption and diffusion of Chatbot Technology in the German insurance sector.

[18] Alalwany, E., & Mahgoub, I. (2024). Security and trust management in the internet of vehicles (IoV): Challenges and machine learning solutions. Sensors, 24(2), 368.

[19] Abbasi, B., Khanmohammadi, M., Moradi, Z., & Mahmoodiyan, T. (2019). Capacity building of green accounting consequences based on the explanation of strategic management accounting techniques. Iranian Journal of Finance, 3(4), 23-59.

[20] Göktepe Körpeoğlu, S., & Göktepe Yıldız, S. (2023). Comparative analysis of algorithms with data mining methods for examining attitudes towards STEM fields. Education and Information Technologies, 28(3), 2791-2826.

[21] Breilin, S. (2022). Comparison of Blockchain technology in various segments of supply chain management.

[22] Schardong, F., & Custódio, R. (2022). Self-sovereign identity: a systematic review, mapping and taxonomy. Sensors, 22(15), 5641.

[23] Turi, A. N. (2023). Financial Technologies and DeFi. A Revisit to Digital Financial Revolution.

[24] Platania, S. A. (2023). The state-of-the-art of the research methodology on blockchain technology: proposal for a research agenda and policy implications.

[25] Tran, K. P. (Ed.). (2022). Machine Learning and Probabilistic Graphical Models for Decision Support Systems. CRC Press.

[26] Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. Journal of planning education and research, 39(1), 93-112.