Journal of Contemporary Perspectives in Accounting & Digitalization
Vol. 7, No. 1, December 2024, pp. 44-54
DOI: https://doi.org/10.4038/jcpad.v7i1.21

Department of Accounting
Faculty of Management Studies and Commerce
University of Sri Jayewardenepura, Sri Lanka

AUDITOR'S PERCEPTION ON THE LEVEL OF USAGE AND IMPORTANCE OF FRAUD DETECTION AND PREVENTION THROUGH SOFTWARE-BASED METHODS: EVIDENCE FROM SRI LANKA

✉ ✉
Fernando I, Manawadu I
Department of Accounting, University of Sri Jayewardenepura

ABSTRACT

The increasing number of fraudsters and the challenges of fraud recognition and mitigation have made it crucial for businesses to adopt modern fraud identification and prevention systems. Traditional methods are no longer sufficient, and modern fraudulent actions require sophisticated tactics for prevention and detection. Organisations must now employ software-based fraud detection and avoidance procedures to detect and prevent fraud in real time. This study aims to determine the usage and significance of software-based fraud prevention and identification approaches from the perspectives of auditors in Sri Lanka, a developing country during an economic crisis. Further, this study investigates the challenges faced by Sri Lankan businesses in integrating Information Technology (IT) in this area. A quantitative research approach was used, and primary data was gathered using a self-administered questionnaire. The study's sample included 104 internal and external auditors. Major findings from this study include that software-based fraud prevention techniques like firewalls, password protection, and virus scanning are the most popular and highly effective, while sophisticated techniques like genetic algorithms, K nearest neighbours, and random forests have the opposite effect. The study reveals that Sri Lankan businesses face challenges in fraud detection and prevention due to lack of knowledge, training, and evolving fraud patterns. The findings also reveal significant differences in perceptions between male and female auditors regarding the usage and importance of fraud prevention and detection tools, as well as specific challenges associated with their implementation. The findings aim to promote software-based methods among policymakers and practitioners to overcome implementation challenges.

Keywords: Challenges of Implementation, Forensic Accounting, Frauds, Software-based Methods

Received:	Accepted revised version:	Published:
01.03.2024	15.10.2024	10.12.2024

Suggested citation: Fernando, I & Manawadu, I 2024, 'Auditor's perception on the level of usage and importance of fraud detection and prevention through software-based methods: evidence from Sri Lanka', *Journal of Contemporary Perspectives in Accounting and Digitalization*, vol. 7, no. 1, pp. 44-54.

✉ isurianjalika@gmail.com
✉ isurumanawadu@sjp.ac.lk

1 INTRODUCTION

Fraud and corruption are pervasive threats to organizations and individuals, deeply rooted in human behavior. These illicit activities, often concealed by their perpetrators, continue to pose significant challenges in detection and prevention (Bănărescu 2015). The global rise in corporate fraud rates underscores the growing importance of forensic accounting, providing accountants and professionals with opportunities to think innovatively about fraud prevention and detection (Peiris & Aruppala 2021). Economic recessions exacerbate fraudulent activities, while technological advancements, particularly through the internet, have enabled more sophisticated methods of corruption. Although statistical and Machine Learning (ML) technologies have demonstrated efficacy in combating fraud, resourceful fraudsters often find ways to bypass these systems.

In response to the heightened risks of fraud during economic downturns, organizations must adopt robust anti-fraud strategies to safeguard their financial performance and credibility. The integration of advanced IT systems is essential in this data-driven era, where fraudsters constantly adapt to evolving detection methods. Thus, developing adaptable and dynamic fraud detection models has become a necessity. This study seeks to address these challenges by providing valuable insights to enterprises, financial institutions, and policymakers to enhance system security and strengthen fraud protection mechanisms.

The primary objective of this research is to explore auditors' perceptions of the usage, importance, and challenges associated with software-based fraud detection and prevention methods in Sri Lanka. Specifically, it examines how auditors view these methods in terms of their usage, significance and challenges to their adoption. Additionally, the study investigates the perceived differences between male and female auditors regarding the usage, significance and challenges of software-based fraud prevention tools, thereby contributing to the broader discourse on gender diversity and its impact on organizational processes.

Despite the global adoption of technologies such as Artificial Intelligence (AI) and blockchain in fraud prevention, their implementation in Sri Lanka remains limited. This gap hinders the financial sector’s ability to mitigate fraudulent activities effectively, impacting financial performance and customer trust. Previous studies have emphasised the need for greater adoption of these technologies, highlighting the lack of adequate mechanisms within Sri Lanka's financial organisations to monitor and prevent fraud (Rathnakrishnan & Baskar 2024, Cao et al., 2024). By examining these issues, this study aims to bridge critical research gaps, particularly given that most prior studies on fraud prevention techniques have focused on developed nations, leaving the Sri Lankan context underexplored.

The findings of this research are expected to provide actionable recommendations for enhancing the adoption and effectiveness of software-based fraud detection methods in Sri Lanka. By analysing the challenges faced in implementation and the significance of these methods through auditors' gendered perceptions, this study seeks to promote the importance of IT-driven fraud prevention among policymakers and practitioners. Ultimately, it aspires to contribute to the development of more resilient and adaptive fraud detection strategies, fostering trust and integrity in Sri Lankan enterprises, particularly within the finance and e-commerce sectors.

The remaining sections of the study are structured as follows; the next section discusses the existing literature; the third section elaborates on the research methodology; the fourth section represents the analysis and discussion, and the conclusion is presented in the last section.

2 LITERATURE REVIEW

In this section, previous research is reviewed and summarised along with its major concepts, body of knowledge, and empirical gaps.

Financially motivated fraudsters engage with companies through internal or external means, involving managers and staff in institutional deception (Clifton et al. 2010). External fraudsters, categorised as average offenders, criminal offenders, and organised crime offenders, may act opportunistically, driven by sudden temptations or financial pressures (Clifton et al. 2010). Fraudulent accounting disclosure and asset mismanagement led to increased costs for businesses (James et al. 2006). To effectively prevent and detect corporate fraud in Sri Lanka, it is strongly recommended to implement robust fraud prevention and detection techniques, including advanced software solutions (Peiris & Aruppala 2021). Studies by Othman et al. (2015) highlight the prevalence of fundamental fraud prevention measures such as password protection, firewalls, and virus protection in organisations, while noting the infrequent use of punitive systems. Omar et al. (2012) find that internal audit and fraud investigation departments are less impactful for fraud prevention in a Malaysian government agency. Gupta and Singh (2012) advocate for decision trees in identifying accounting fraud, while Bierstaker et al. (2006) note external auditors' use of various standard techniques against fraud.

Current studies on financial fraud detection primarily rely on financial statement numbers, making it challenging to distinguish between fraudulent and legitimate data due to intentional concealment. Recognising the importance of textual information, recent research emphasises its utility in fraud detection, particularly given that a significant portion of financial reporting involves textual explanations of numerical data (Dong et al. 2014). Expected attribute sample shape with zero error rates. It calculates the proportion of the population that possesses a particular trait or quality. The sampling procedure is stopped, and the error or fraud is investigated if a sizable error or fraud is discovered in the sample.

The method of finding patterns in huge data sets by combining techniques from statistics, ML, and databases. Data mining is, in other words, the stage of knowledge discovery and database analysis. Data mining-based fraudulent financial diagnosis is a relatively similar problem affecting other categorisation complications. When identifying malpractice, for instance, it can be difficult to select the appropriate characteristics, fine-tune the specifications, and assess the problem (West et al. 2016).

The complexity of fraud analysis in a digital environment has increased with the development of innovations and technologies like blockchain, robotics, and AI (Oladejo & Jack 2020). Using automated tools and processes continues to be the largest challenge. To prevent and detect fraudulent actions and to support deliberate managerial decisions, it is imperative to analyse opportunities for the expansion and integration of new models and computerised systems (Banarescu 2015). The possibility of early fraud alerting is increased using proactive techniques and real-time processing greatly shortens the time window for conducting computational analysis and arriving at a reliable fraud decision in response to recently arrived system events (Edge & Falcone 2009).

3 RESEARCH DESIGN AND METHODS

This section discusses the study's population and sample, research approach, data collection methods, and data analysis techniques.

3.1 Research Approach

Employing a quantitative research approach, this study investigates auditors' perceptions regarding the extent of utilization and the significance of software-based fraud prevention and detection methods in Sri Lankan organizations. Additionally, it aims to explore perceptual differences between male and female auditors concerning the usage, significance, and associated challenges of these methods. A quantitative approach facilitates a systematic examination of the degree of adoption, importance and the challenges encountered in implementing software-based fraud detection and prevention techniques.

3.2 Population and Study Sample

In this study, the population consists of qualified internal and external auditors in Sri Lanka, including those working for the Big Four audit firms, other audit firms, and internal audit divisions within organisations. Internal auditors include those who perform in the internal audit function of organisations in various industries, while external auditors include those who are at the supervisory level, managerial level, or above and associated with the auditing process in various organisations for their distinctive attributes or their observations, sentiments, or preconceptions.

3.3 Sample Size and Selection of Sample, Sampling Method

Correspondingly, the survey research design, non-probability sampling procedure, was applied to choose a representative sample of 104 internal and external auditors. The data collection and processing resources, enable a sufficiently large data set to examine various perspectives on fraud detection and prevention through software-based methods. The decision to use non-probability sampling aligns with the study's focus on obtaining insights from auditors who possess specific qualifications and experiences relevant to the research topic. By targeting auditors involved in both internal and external auditing roles across various industries, the sampling criteria aim to capture a broad spectrum of perspectives on the usage and significance of fraud detection and prevention software in Sri Lanka.

3.4 Sources and Collection of Data

A questionnaire developed to gather primary data for the research was based on a comprehensive literature review that included prior similar studies (Jayasinghe & Ajward 2019). There are various questions on the survey including Likert-scale questions. Further to that, the questionnaire was validated by a few professionals, such as a senior lecturer at a university with research experience and a senior manager and compliance department manager at a well-known bank in Sri Lanka.

Additionally, respondents were informed at the beginning of the survey that their privacy and confidentiality would be safeguarded, encouraging them to provide honest and candid responses. The questionnaire was divided into four sections: the first section collected

demographic information to better understand the sample; and the second section comprised mainly multiple-choice questions on the use of software techniques for fraud prevention in Sri Lanka. The third and fourth sections used a five-point Likert scale to assess the perceived significance of these techniques and the challenges associated with their implementation.

3.5 Data Analysis Strategies

The data analysis was conducted thoroughly, with the auditors' responses evaluated using the Statistical Package for Social Sciences (SPSS). To achieve the research objectives, descriptive analysis was employed, and the usage of fraud detection methods was assessed through mean ranking. Independent sample t-tests and one sample t-tests were also utilised.

4 ANALYSIS AND DISCUSSION

The study's findings and discussion describe the demographic variables of the above-mentioned selected sample and clarify the most used software-based fraud recognition and prevention techniques. Furthermore, this section examines the significance of those methods based on auditor perceptions of some demographic characteristics. The findings of the analysis are derived from a descriptive analysis, as specified in the data analysis strategies, to achieve the research objectives.

4.1 Descriptive Statistics

4.1.1 Mostly used software-based techniques for fraud detection and prevention

To address the first objective of the study—identifying the most commonly used software tools in Sri Lanka—Table 1 presents 21 software-based techniques along with their descriptive statistics, including mean rankings.

Table 1: Mostly used Software-based Methods for Fraud Detection and Prevention

Software Tool	Male Auditors			Female Auditors			Total		
	Mean	Std. Deviation	Mean Rank	Mean	Std. Deviation	Mean Rank	Mean	Std. Deviation	Mean Rank
1. Virus Protection	2.98	0.15	1	2.98	0.13	1	2.98	0.14	1
2. Password Protection	2.98	0.15	2	2.98	0.13	2	2.98	0.14	2
3. Firewalls	2.98	0.15	3	2.95	0.29	3	2.96	0.24	3
4. Financial Ratios	2.93	0.33	4	2.95	0.29	4	2.94	0.31	4
5. Digital Analysis	2.84**	0.43	6	2.82**	0.50	6	2.83**	0.47	5
6. Decision Trees	2.77**	0.52	9	2.83**	0.46	5	2.81**	0.48	6
7. Continuous Auditing	2.89**	0.32	5	2.73**	0.52	7	2.80**	0.45	7
8. Benford’s Law	2.84**	0.48	7	2.73**	0.61	8	2.78**	0.56	8
9. Filtering Software	2.80**	0.51	8	2.70**	0.62	9	2.74**	0.57	9
10. Data Mining	2.77**	0.48	10	2.57**	0.62	11	2.65**	0.57	10
11. Discovery Sampling	2.73**	0.50	11	2.58**	0.70	12	2.64**	0.62	11
12. Neural Networks	2.70**	0.59	12	2.57**	0.65	10	2.63**	0.63	12
13. Logistic Regression	2.66**	0.57	13	2.50**	0.68	14	2.57**	0.63	13
14. Discriminant Analysis	2.52	0.59	15	2.53	0.65	13	2.53	0.62	14

15. Hybrid Decision Support System	2.52**	0.63	14	2.48	0.60	15	2.50**	0.61	15
16. Bayesian Networks	2.45**	0.66	16	2.33**	0.68	16	2.38**	0.67	16
17. Clustering based Method	2.27**	0.59	17	2.28	0.58	17	2.28	0.58	17
18. Random Forest	2.23*	0.57	19	2.27	0.63	18	2.25**	0.60	18
19. Support Vector Machine	2.25**	0.53	18	2.17**	0.59	19	2.20**	0.56	19
20. K Nearest Neighbours	2.20**	0.55	20	2.13**	0.62	20	2.16**	0.59	20
21. Genetic Algorithm	2.18**	0.54	21	2.10**	0.60	21	2.13**	0.58	21

Based on the one sample t-test performed, the significance of the difference between the test value of 3 and the mean values are also indicated, where $^{**}p<.01$ and $^{*}p<.05$.

Table 1 presents key findings on software-based fraud recognition and prevention methods in Sri Lankan organisations, derived from descriptive statistics and one sample t-tests. Notably, virus protection, password protection, and firewalls share the highest mean value (2.98), indicating their widespread use among male auditors. Financial ratios, continuous auditing, digital analysis, Benford's law, and filtering software follow closely in usage.

Accordingly, based on the overall ranking, virus protection, password protection, firewalls, financial ratios, and digital analysis emerge as the top five tools. Conversely, the Genetic Algorithm, K Nearest Neighbours, Support Vector Machine, Random Forest, and Clustering based method are the least used. According to Peiris and Aruppala (2021) filtering software, virus protection, and firewalls are among the most regularly utilised fraud prevention and detection tools in Sri Lanka.

The results highlight a gap in the adoption of globally prevalent ML methods in Sri Lanka, potentially due to some respondents' lack of familiarity with these software methods.

4.1.2 Perception difference between male and female auditors on mostly used software-based fraud detection and prevention techniques

According to the not tabulated independent sample t-test, there is a significant difference in perceptions of male auditors and female auditors. Some of the results such as data mining (mean difference: 0.206), continuous auditing (mean difference: 0.153), Bayesian networks (mean difference: 0.121) and logistic regression (mean difference 0.159) have more perception differences among male and female auditors. In conclusion, there is a significant perception difference between male and female auditors on mostly used software tools.

4.2 Significance Level of Software-based Fraud Detection and Prevention Methods

This section of data analysis describes how to achieve the second objective of the study, to assess the significance level of fraud detection and prevention software-based methods in Sri Lanka as per the perceptions of auditors based on their gender. One sample test was performed, and those results and the descriptive statistics are presented in Table 2 to identify and list the most significant and the least significant methods. Participants were asked to score the methods from most significant to insignificant to gather data using the Likert scale.

Table 2: Importance of Software-based Fraud Detection and Prevention Methods

Software Tool	Male Auditors			Female Auditors			Total		
	Mean	Std. Deviation	Mean Rank	Mean	Std. Deviation	Mean Rank	Mean	Std. Deviation	Mean Rank
1. Password Protection	3.95**	0.75	1	4.05**	0.65	1	4.01**	0.69	1
2. Virus Protection	3.95**	0.75	2	4.00**	0.67	2	3.98**	0.70	2
3. Firewalls	3.86**	0.70	3	3.93**	0.69	3	3.90**	0.69	3
4. Financial Ratios	3.82**	0.54	4	3.83**	0.79	6	3.83**	0.69	4
5. Digital Analysis	3.66**	0.78	9	3.93**	0.66	9	3.82**	0.72	5
6. Filtering Software	3.80**	0.70	5	3.82**	0.62	4	3.81**	0.65	6
7. Continuous Auditing	3.72**	0.67	6	3.85**	0.66	7	3.80**	0.66	7
8. Data Mining	3.68**	0.77	7	3.75**	0.54	5	3.72**	0.65	8
9. Discovery Sampling	3.68**	0.74	8	3.70**	0.85	8	3.69**	0.80	9
10. Decision Trees	3.64**	0.72	11	3.63**	0.66	10	3.63**	0.68	10
11. Benford's Law	3.59**	0.73	13	3.67**	0.66	15	3.63**	0.68	11
12. Neural Networks	3.66**	0.83	10	3.58**	0.81	11	3.62**	0.82	12
13. Discriminant Analysis	3.61**	0.81	12	3.55**	0.79	12	3.58**	0.80	13
14. Bayesian Networks	3.52**	0.85	14	3.58**	0.70	13	3.55**	0.76	14
15. Logistic Regression	3.35**	0.81	18	3.58**	0.70	18	3.48**	0.75	15
16. Hybrid Decision Support System	3.43**	0.76	15	3.51**	0.75	14	3.48**	0.75	16
17. Clustering based Method	3.41**	0.84	16	3.52**	0.70	17	3.47**	0.76	17
18. Support Vector Machine	3.36**	0.78	17	3.22**	0.67	16	3.28**	0.72	18
19. K Nearest Neighbours	3.25**	0.72	19	3.15**	0.71	20	3.19**	0.71	19
20. Random Forest	3.23**	0.74	20	3.15**	0.76	19	3.18**	0.75	20
21. Genetic Algorithm	3.18	0.69	21	3.08	0.70	21	3.13	0.69	21

Based on the one sample t-test performed, the significance of the difference between the test value of 3 and the mean values are also indicated, where $^{**}p<.01$ and $^{*}p<.05$

Password protection emerges as the most crucial method for fraud prevention, with a mean ranking of 4.01, unanimously recognised by both genders. Other highly significant tools include virus protection, firewalls, financial ratios, digital analysis, filtering software, and continuous auditing.

While there is a slight gender-based perception difference in middle rankings, both male and female auditors prioritise the same methods as most and least significant. Notably, both groups highly value password protection, with male auditors assigning a mean ranking of 3.95 and female auditors of 4.05. Decision trees, neural networks, data mining, and discovery sampling also hold significance but rank lower.

The mean rankings indicate that discriminant analysis, bayesian networks, logistic regression, hybrid decision support system, and clustering are among the least significant methods. Support vector machine, K nearest neighbours, random forest, and genetic algorithm are deemed the least important tools for fraud prevention.

4.2.1 Perception Difference between Male and Female Auditors on Significance Level of Software-based Fraud Detection and Prevention Techniques

There is a significant perception difference between male auditors and female auditors as per the independent t-test results (not tabulated). Neural networks (mean difference: 0.076),

discriminant analysis (0.064), decision trees (mean difference: 0.003), support vector machine (mean difference: 0.147), genetic algorithm (mean difference: 0.098) and random forest (mean difference: 0.077) are some of the software-based methods that have a mean difference on significance levels. The results interpret that there is a perception difference of male and female auditors on the significance level of the software tools.

4.3 Challenges in Using Software-based Methods for Fraud Detection and Prevention in Sri Lanka

The final objective of the research is to identify the challenges to using software-based methods in Sri Lanka. From selected challenges identified from an in-depth review, descriptive statistics, mean ranking and one sample t-test are performed and according to the results, Table 3 depicts, what are the most challenging to the organisations in Sri Lanka as most of the tools used in other countries to simplify the fraud investigation procedures.

Table 3: Descriptive Statistics- Challenges to Using Software-based Methods in Sri Lanka

	Male auditors			Female auditors			Total		
Challenges	**Mean**	**Std. Deviation**	**Mean Rank**	**Mean**	**Std. Deviation**	**Mean Rank**	**Mean**	**Std. Deviation**	**Mean Rank**
1. Lack of knowledge of software-based fraud detection and prevention methods	4.34**	0.68	3	4.33**	0.68	1	4.34**	0.68	1
2. Change in fraud patterns	4.43**	0.70	1	4.27**	0.76	3	4.34**	0.73	2
3. Lack of training in software-based fraud detection methods or fraud investigation techniques	4.36**	0.78	2	4.30**	0.74	2	4.33**	0.76	3
4. High implementation, upgrade and maintenance costs	4.25**	0.75	5	4.23**	0.77	5	4.24**	0.76	4
5. Lack of proper infrastructure	4.30**	0.73	4	4.20**	0.73	6	4.24**	0.73	5
6. Risk of data leaks	4.18**	0.69	6	4.25**	0.63	4	4.22**	0.65	6

Source: Author Constructed

Table 3 highlights challenges faced by Sri Lankan organisations in implementing software tools for fraud detection and prevention, based on auditor perceptions. Female auditors identify a lack of knowledge of software-based methods as the most challenging (4.33), while male auditors see changing fraud patterns as their primary obstacle (4.43). Both groups agree on the difficulty of inadequate training, though with slight mean value differences. Overall, the risk of data leaks is the least challenging (4.22), while a lack of knowledge stands out as the most significant hurdle (4.34), emphasising the need for addressing these challenges to integrate IT into organisational systems effectively. As per previous studies, fraud protection and detection software is not affordable, a major portion of data is not incorporated into databases, and not all text files are included in the final reports (Banarescu 2015). While organisations may be hesitant to invest in anti-fraud technology, the perceived benefits of the software may outweigh the cost due to its effectiveness (Bierstaker et al. 2006).

4.3.1 Perception difference between male and female auditors on challenges to use software-based methods in Sri Lanka

The last objective is achieved, and the perception difference is presented according to the independent t-test results which are not tabulated. Change of fraud patterns (mean difference: 0.165), lack of proper infrastructure (mean difference: 0.095), lack of training in software-based fraud detection methods or fraud investigation techniques (mean difference: 0.064) and lack of knowledge on software-based fraud detection and prevention methods (mean difference: 0.008) have only perception difference that proves that there is a perception difference among the two male and female groups but it is only a slight difference.

5 CONCLUSION

This study aimed to explore software-based fraud detection and prevention methods in Sri Lanka, focusing on three key objectives: assessing the usage and significance of these methods, identifying the challenges associated with their implementation, and examining significant differences between male and female auditors in terms of their perceptions of usage, significance, and challenges.

The findings reveal that traditional software-based tools, such as virus protection, password protection, and firewalls, are the most widely used and considered highly significant by auditors. These methods are valued for their simplicity and ease of implementation, making them suitable for organizations with limited technical expertise or resources. However, advanced techniques, such as genetic algorithms, random forests, and K-nearest neighbors, are underutilized, highlighting a gap in technological adoption. The lower usage of these sophisticated methods points to a need for enhanced training and knowledge dissemination to enable their integration into fraud prevention practices.

The study also identifies several challenges that hinder the adoption of advanced fraud detection methods in Sri Lanka. Key challenges include a lack of knowledge about these methods, insufficient training in fraud detection techniques, high costs associated with implementation and maintenance, and inadequate infrastructure. Additionally, evolving fraud patterns pose a dynamic challenge, requiring organizations to adopt more adaptive and proactive strategies. These findings align with global studies that emphasise the importance of IT-driven solutions in combating sophisticated fraud but highlight unique barriers in the Sri Lankan context.

A critical aspect of this study is its examination of gender-based differences in perceptions of fraud detection methods. Male and female auditors largely agree on the significance of traditional software-based tools like password protection and virus protection. However, their perceptions diverge slightly regarding advanced methods, such as neural networks and logistic regression, and on challenges, including the impact of evolving fraud patterns and infrastructure limitations. These differences suggest that gender diversity may influence how technology is perceived and adopted within organisations, adding a nuanced layer to the understanding of technological integration in fraud prevention.

This research highlights the critical role of software-based fraud detection methods in strengthening organizational resilience against fraud. While traditional tools remain the cornerstone of fraud prevention in Sri Lanka, addressing the identified challenges is essential for fostering the adoption of advanced techniques. Policymakers, practitioners, and

organizations should prioritize targeted capacity-building initiatives, infrastructure development, and policy interventions to overcome these barriers. Moreover, understanding gender-based perceptual differences can guide more inclusive strategies for implementing fraud detection tools.

In conclusion, this study underscores the need for Sri Lankan organizations to bridge the gap between traditional and advanced fraud detection methods. By addressing challenges and leveraging diverse perspectives, organizations can enhance their fraud prevention capabilities, align with global best practices, and foster trust and efficiency in their operations. This research contributes valuable insights into the Sri Lankan context, providing a foundation for future studies to explore the integration of cutting-edge technologies and their impact on organizational performance in similar settings.

REFERENCES

Ajzen, I 1991, 'The theory of planned behaviour', *Organisational Behaviour and Human Decision Processes*, vol. 50, no. 1, pp. 179–211.

Bănărescu, A 2015, 'Detecting and preventing fraud with data analytics', *Procedia Economics and Finance*, vol. 32, no. 32, pp. 1827–1836.

Bierstaker, JL, Brody, RG & Pacini, C 2006, 'Accountants' perceptions regarding fraud detection and prevention methods', *Managerial Auditing Journal*, vol. 21, no. 5, pp. 520–535.

Cao, J, Kristanto, AB, & Gu, Z 2024, 'Evolution of research streams and future research directions in accounting education: quantitative systematic literature review', *Issues in Accounting Education*, vol. 39, no. 4, pp. 1-35.

Clifton, J & Snyder, H 2010, 'Forensic accounting fieldwork, media and exercises project', *Journal of Forensic & Investigative Accounting,* vol. 2, no. 2, pp.294-307

Dong, W, Liao, SS, Fang, B, Cheng, X, Chen, Z & Fan, W 2014, 'The detection of fraudulent financial statements: an integrated language model', *Pacific Asia Conference on Information System*s, p. 383.

Edge, ME & Falcone, SPR 2009, 'A survey of signature-based methods for financial fraud detection', *Computers & Security,* vol. 28, no. 6, pp. 381-394.

Gupta, R, & Singh GN 2012, 'A data mining framework for prevention and detection of financial statement fraud', *International Journal of Computer Applications*, vol. 50, no. 8, pp. 7-14.

Jans, M, Lybaert, N & Vanhoof, K 2010, 'Internal fraud risk reduction: results of a data mining case study', *International Journal of Accounting Information Systems*, vol. 11, no. 1, pp. 17-41.

Jayasinghe, D & Ajward, R 2019, 'The level of usage and importance of fraud detection and prevention techniques used in Sri Lankan banking and finance institutions: perceptions of internal and external auditors', *CA Journal of Applied Research*, vol. 3, no. 1, pp. 158–180.

KPMG 2009, *KPMG Malaysia fraud, bribery and corruption survey 2009*. Kuala Lumpur: KPMG Forensic.

KPMG 2013, *KPMG Malaysia fraud, bribery and corruption survey 2013*. KPMG.

Meitriana, MA, Suwena, IKR & Indrayani, L 2019, 'The influence of fraud triangle and theory of planned behaviour on students' academic fraud in Bali', *3rd International Conference on Tourism, Economics, Accounting, Management, and Social Science*. Atlantis Press.

Oladejo, MT & Jack, L 2020, 'Fraud prevention and detection in a blockchain technology environment: challenges posed to forensic accountants', *International Journal of Economics and Accounting,* vol. 9, no. 4, pp. 315.

Omar, N, Maria, K, Bakar, A & Bakar, KM 2012, 'Fraud prevention mechanisms of Malaysian government-linked companies: an assessment of existence and effectiveness', *Journal of Modern Accounting and Auditing*, vol. 8, no. 1, pp.15-31.

Othman, R, Aris, NA, Mardziyah, A, Zainan, N & Amin, NM 2015, 'Fraud detection and prevention methods in the Malaysian public sector: accountants' and internal auditors' perceptions', *Procedia Economics and Finance*, vol. 28, pp. 59–67.

Peiris, GK & Aruppala, WD 2021, 'A study on fraud prevention and detection methods in Sri Lanka', *Kelaniya Journal of Management*, vol. 10, no. 2, pp. 37–56.

West, J & Bhattacharya, M 2016, 'Intelligent financial fraud detection: a comprehensive review', *Computers and Security*, vol. 57, pp. 47–66.