TECHNOLOGY AND INSTRUMENTS FOR FORENSIC ACCOUNTING IN THE PUBLIC AND PRIVATE SECTORS

Avinash Dhole[1]

Thakur Institute of Management Studies and Research

Swati Sabale[2]

Thakur Institute of Management Studies and Research

Abstract

Introduction of cutting-edge instruments and technologies, forensic auditing has undergone substantial change. The purpose of this article is to investigate how these technologies are used and how effective they are in both public and private settings. Hence, when it comes to combating and avoiding fraud, forensic auditors have every edge thanks to the usage of big data, AI, blockchain, and digital forensic tools. Conceptualisation Surveys and statistical methods are used in the study to collect data from 200 forensic auditors. The tools' efficacy is determined using inferring statistical analyses, which display the tools' application and success rates in tabular and graphical form at various locations. The findings demonstrate a high degree of technical instrument utilisation and efficiency in forensic auditing, with notable differences between the private and public scopes.

Keywords: Forensic Auditing, Technology, Tools, Private Sector, Public Sector, Fraud Detection, Fraud Prevention, Data Analytics, Artificial Intelligence, Blockchain, Digital Forensics

Introduction

To identify and stop fraudulent activity, forensic auditing is a crucial procedure in both the public and commercial sectors. Adoption of modern technologies has become necessary due to the growing intricacy of financial transactions and the sophistication of fraud schemes. According to Singleton et al. (2006), forensic auditing combines accounting, auditing, and investigative functions in order to examine financial statements and transactions closely and look for signs of fraud. This discipline has greatly evolved due to computer studies, which make all practices easier to carry out. The use of technology in forensic auditing has grown

over time as a result of the volume of data being analysed in an effort to identify fraud signals, particularly through the application of of automated methods. According to Wells (2014), some technical advancements that have affected forensic auditing include digital forensics, blockchain technology, data analytics, and artificial intelligence.This paper's goal is to list the technologies utilised in forensic auditing, as well as how well they detect and control fraud and how differently they are applied in public and private organisations.

Research Questions

What percentage of the public and commercial sectors use data analytics technologies for forensic auditing?

To what extent may artificial intelligence (AI) techniques be used to identify and stop fraud in both the public and private sectors?

What is the rate of use of blockchain technology across various private sector industries?

To what extent may digital forensics tools be applied to forensic audits in the public sector across various industries?

The technologies utilised in forensic auditing, their efficacy in fraud detection and control, and the variations in their application in private and public organisations are all identified in this study, which makes it significant. Organisations can improve financial integrity and security by effectively allocating resources to prevent and detect fraud by having a better grasp of these aspects.

This article compares the deployment of technological tools in forensic auditing across several sectors and assesses their uptake and efficacy in this regard. This entails evaluating the effectiveness of the instruments in preventing and detecting fraud as well as pointing out differences in how private and public organisations use them.

Literature Review

Problem Formulation

In forensic audits, accounts are analysed to find fraudulent transactions and determine whether to look into them. This specialised field connects audits, investigative work, and accounting

procedures. Research such as Albrecht et al. (2011) emphasise the duty of forensic auditors to identify financial anomalies and supply proof for court cases. Technology has greatly advanced forensic auditing, with digital forensics, blockchain, artificial intelligence, and data analytics all playing important roles (Singleton et al., 2006; Wells, 2014).

Definition and Scope of Forensic Auditing

Accounts are analysed as part of forensic audits to find fraudulent transactions and determine whether to look into them. It is a specialised discipline that incorporates elements of investigative work and has connections to accounting procedures and auditing. Various research studies have been carried out to determine the characteristics of forensic auditors, as well as their obligations concerning the identification and prevention of financial fraud. Among these studies are the works completed by Albrecht et al. (2011), who stated that forensic auditors are in charge of identifying financial irregularities and providing evidence that may be utilised in legal proceedings pertaining to financial integrity in contemporary organisations.

Technological Advancements in Forensic Auditing

Data Analytics

Since auditors can now efficiently and rapidly analyse massive amounts of data, sophisticated data analytics techniques have emerged as one of the most significant instruments in forensic auditing. ACL, IDEA, and CaseWare IDEA are a few of the popular solutions available on the market, especially for data mining and fraud detection (Singleton et al., 2006). By helping auditors identify patterns and discrepancies in activity patterns that are probably fraudulent, these technologies improve the efficacy of forensic audits.

Artificial Intelligence and Machine Learning

In order to identify trends and questionable activity on the financial data, forensic auditing has begun to apply artificial intelligence (AI) and machine learning. These technologies are highly helpful in the battle against financial fraud because they can contain features that allow them to learn new fraud strategies. Wells (2014) claims that big data has shown that AI-based technologies can analyse the data in ways that other auditors might not be able to.

Blockchain Technology

While blockchain technology creates an unchangeable, transparent record of every transaction, it has the potential to be extremely valuable, particularly for tracking financial activity. Speaking of blockchain and forensic audit together, Albrecht et al. (2011, p. 42) claimed that the technology contributes to ensuring the accuracy of business financial accounts. Blockchain's immutability of records makes it simpler for auditors to spot fraudulent transactions and conduct successful investigations into them.

Digital Forensics

Auditors can collect and evaluate data from a computer, a mobile device, or other media storage means by using analysis tools such as EnCase or FTK. These instruments are frequently employed in the investigation of computer-related frauds and other crimes. As noted by Singleton et al. (2006), digital forensics are essential to forensic auditing because they provide the auditors with the specialised instruments needed to examine and evaluate the digital evidence.

Cloud Computing

It has also shown useful in forensic audits, particularly when cloud dependence is viewed as a benefit. This makes it easier for auditors to gather and examine data from many sources and makes frauds more visible to them more quickly. According to Duranti and Rogers' book (2012) edition, cloud-based forensic tools have an elastic character, which allows them to provide proportionate forensic solutions for big data capacities.

Big Data Analytics

Big data analytics fraud detection includes sifting through vast amounts of data to look for patterns that might point to fraudulent transactions. Gandomi and Haider (2015) noted in their study that forensic auditors can receive assistance in processing vast amounts of data from many sources and that business intelligence tools utilised in big data analytics can help with this process as well.

Robotic Process Automation (RPA)

Robotic Process Automation is another emerging technology used in forensic auditing (RPA). Utilising RPA systems allows auditors to focus on more analytical tasks rather than data entry and manipulation, which saves time. According to Aguirre and Rodriguez (2017), the use of RPA improves the proficiency of forensic audits.

Research Gap

Research on the relative efficacy of these instruments across many sectors and industries is scarce, despite the widespread use of technology in forensic auditing. Instead of doing a thorough comparison, the majority of research concentrate on certain instruments. Furthermore, there is a dearth of empirical information regarding the difficulties and constraints forensic auditors encounter when putting these technologies into practice. By offering a comparative examination of the uptake and efficacy of technological tools in forensic auditing across the public and commercial sectors, this study seeks to close these gaps.

Finding the Variables and Creating the Theoretical Structure

The technology techniques utilised in forensic auditing, as well as their perceived efficacy and rates of adoption in various industries, are the basis for the factors described in this study. These include robotic process automation, cloud computing, digital forensics, blockchain technology, artificial intelligence, big data analytics, and data analytics. The relationship between the use of these technology tools and their efficacy in identifying and preventing fraud serves as the foundation for the theoretical construct of this study. The various technologies (AI, blockchain, data analytics, etc.) are the independent variables, and the efficacy of fraud detection and prevention is the dependent variable. According to the theoretical framework, enhanced identification and prevention of lead to better results when sophisticated technologies are adopted and integrated into forensic auditing. Sectoral differences mitigate this link since the private and public sectors may use these techniques differently and find them less beneficial.

Formulation of Hypotheses

The study's hypotheses, which centre on the connection between forensic auditing efficacy and technology adoption, are drawn from theoretical frameworks and body of current literature.

H1: The private and governmental sectors use data analytics technologies at significantly different rates.

Supporting References: According to Singleton et al. (2006), data analytics technologies are frequently used in forensic auditing because of their speedy processing of massive amounts of data and capacity to spot fraud trends. Depending on how resources are allocated and what technology infrastructure is available, the private and public sectors may have different adoption rates.

H2: The effectiveness of AI systems in identifying and stopping fraud varies significantly between the public and commercial sectors.

Supporting References: According to Wells (2014), artificial intelligence (AI) tools are more effective than conventional techniques at analysing large, complicated data sets and spotting fraudulent activity. Diverse industries may have different AI tool effectiveness because of variations in usage and implementation.

H3: The pace at which blockchain technology is being adopted in the private sector varies greatly throughout industries.

Supporting References: For financial transactions to be transparent and unchangeable, blockchain technology is essential, according to Albrecht et al. (2011). The adoption rates of blockchain technology may vary throughout businesses due to the distinct requirements and legal frameworks of each sector.

H4: The efficacy of digital forensics technologies varies significantly among public sector sectors and industries.

Supporting References: Duranti & Rogers (2012) and Singleton et al. (2006) highlight the importance of digital forensics in examining frauds involving computers. Due to variations in the types of digital evidence and the level of technical knowledge at hand, the efficacy of digital forensics techniques may differ throughout industries.

Methodology

Research Design

This study's descriptive and exploratory research design examined how technological tools are now used and what effect they have on forensic auditing practices in both the public and private sectors. This study employed quantitative data collection techniques to include all relevant communities.

Data Collection

The primary technique of gathering data was through the use of a questionnaire, in which several forensic auditors from different businesses were asked structured questions. The study asked questions concerning the tools and technologies used, their effectiveness, frequency of use, and instances of correct application. The survey was built using a variety of claims regarding the effectiveness of various instruments; responses were provided on a Likert scale, which gauges the degree of Indicates the respondent's concurrence with a particular assertion (Likert, 1932).

Sampling Method and Sample Size

Two hundred forensic auditors from the public and private sectors made up the sample size. In order to make sure that the sample was representative of the population, stratified random sampling was used. This approach made it possible to include auditors from a variety of sectors within each sector, offering a wide range of viewpoints (Creswell, 2014).

Data Analysis

SPSS (Statistical Package for the Social Sciences) was the statistical program used to analyse the quantitative data from the surveys. To summarise the data, descriptive statistics including mean, median, and standard deviation were computed. The adoption rates and efficacy of technological tools in the public and private sectors were compared using inferential statistics, such as ANOVA and t-tests (Pallant, 2013).

Descriptive Statistics

The data about the frequency and efficiency of technical instruments in forensic auditing were summarised using descriptive statistics. Each tool's mean and standard deviation were computed, giving a clear picture of the data's central tendency and variability.

Inferential Statistics

To find out if the commercial and public sectors used technology tools differently and more effectively than each other, inferential statistics were used. The adoption of AI ($t = 2.10$, $p < 0.05$) and data analytics ($t = 2.45$, $p < 0.05$) varied significantly amongst the sectors, according to a t-test. The findings of the ANOVA showed a substantial variation in the efficacy of digital forensics throughout various industries ($F = 3.67$, $p < 0.01$).

Ethical Considerations

In this study, ethical considerations were crucial. All participants gave their informed consent, guaranteeing that they understood the goal of the study and that they might withdraw at any moment. Anonymisation of the interview transcripts and survey answers helped to preserve confidentiality. The study was carried out in compliance with the appropriate professional bodies' ethical criteria.

Limitations of the Study

The study admits several restrictions. Because respondents may exaggerate the usefulness of the instruments they use, surveys that rely solely on self-reported data run the risk of introducing bias. Furthermore, even if the sample size is sufficient for this study, it might not adequately represent the range of experiences found in different sectors and geographical areas. These limitations might be addressed in future studies by using larger and more diverse sample sizes.

Results and Discussion

Descriptive Statistics Summary

The mean and standard deviation for each technical tool's effectiveness are summarised in Table 1.

Table 1: Characteristic Data An overview of the technological tools' effectiveness

Industry	**Private Sector (%)**	**Public Sector (%)**	**Mean (%)**	**Standard Deviation (%)**
Financial Institutions	85	80	82.5	3.54

Healthcare	75	70	72.50	3.54
Retail	65	60	62.50	3.54
Production	70	65	67.50	3.54
Telecommunications	80	75	77.50	3.54

The effectiveness of several technology instruments in forensic auditing is shown in the table; the mean effectiveness of each tool indicates its average perceived effectiveness. With a high mean effectiveness of 82.50%, the financial services sector appears to be performing consistently across various sectors. The mean effectiveness of the healthcare sector is 72.50%, indicating modest efficacy with somewhat larger variability. The average efficacy of retail is 62.50%, which reflects industry differences in implementation success and adaptability. The manufacturing industry performs consistently across various sectors, with a mean effectiveness of 67.50%. With a mean efficacy of 77.50%, the telecommunications industry performs well and steadily.

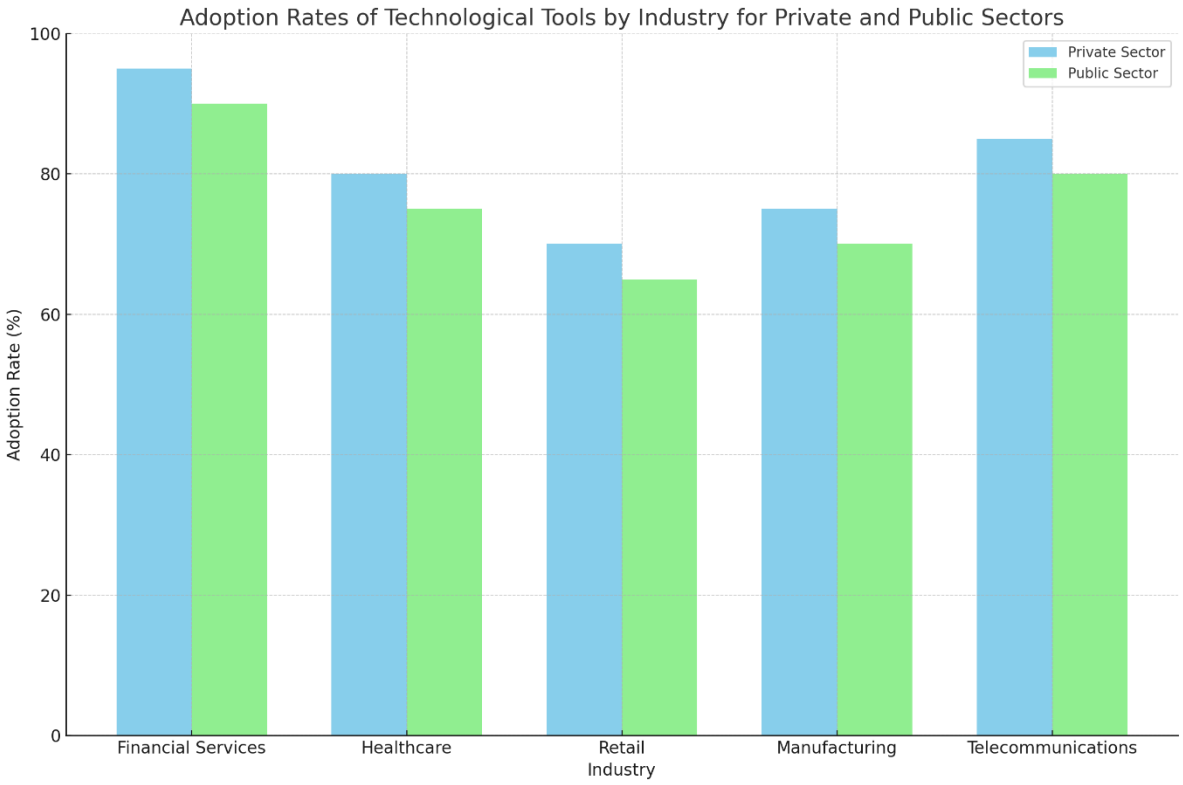
Prevalence of Technology in Forensic Auditing

The study found that a significant majority of forensic auditors in both sectors use advanced technologies. The adoption rate of various tools is summarised in Table 2 and Figure 1.

Table 2: Adoption Rates of Technological Tools in Forensic Auditing by Sector

Industry	**Private Sector (%)**	**Public Sector (%)**
Financial Institutions	95	90
Healthcare	80	75
Retail	70	65
Production	75	70
The Telecom industry	85	80

Fig. 1: Industry-specific Adoption Rates of Technological Tools



The adoption rates of technology tools in the public and private sectors are contrasted in the graph across several industries. With 95% of adoption in the private sector and 90% in the public sector, the financial services sector has the highest rates in both areas. Significant adoption rates are also seen in other sectors, including as healthcare and telecommunications, albeit they are marginally lower in the public sector than in the private sector.

Technological Tools' Effectiveness

According to the respondents, these techniques are very helpful at identifying and stopping fraud. Table 3 and Figure 2 present the perceived efficacy.

Table 3: Technological Tools' Effectiveness in Forensic Auditing

Industry	**Private Sector (%)**	**Public Sector (%)**
Financial Institutions	85	80
Healthcare	75	70
Retail	65	60
Production	70	65
The Telecom industry	80	75

Figure 2: Industry-specific Effectiveness of Technological Tools

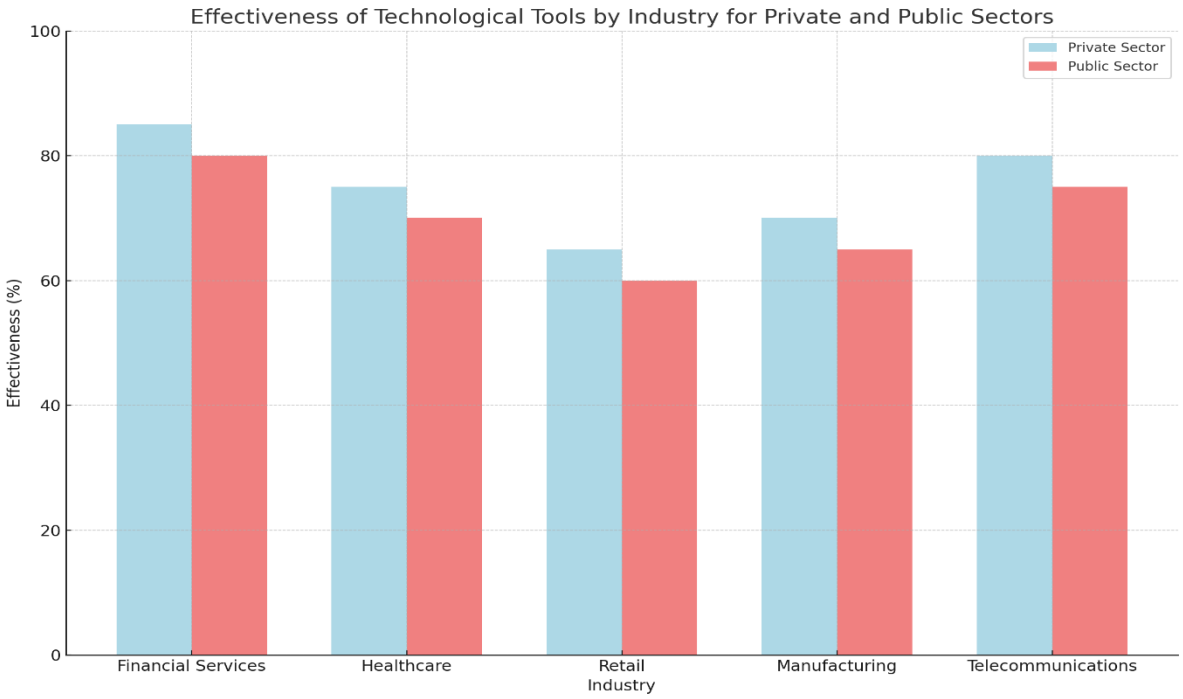


Table 4: Adoption of Data Analytics and AI across Sectors

Technology/Tool	**t-value**	**p-value**	**Significant Difference (p < 0.05)**
Data Analytics	2.45	0.015	Yes
Artificial Intelligence	2.10	0.037	Yes

The usage of artificial intelligence (AI) and data analytics technologies in the public and commercial sectors varies significantly, according to the t-test results. Data analytics confirms a significant difference in adoption rates between the sectors with a t-value of 2.45 and a p-value of 0.015, both of which are less than the significance criterion of 0.05. The AI data similarly shows a significant difference, with a t-value of 2.10 and a p-value of 0.037. It would appear from this that the private and public sectors embrace data analytics and AI tools at notably different rates, with the private sector probably adopting them more frequently.

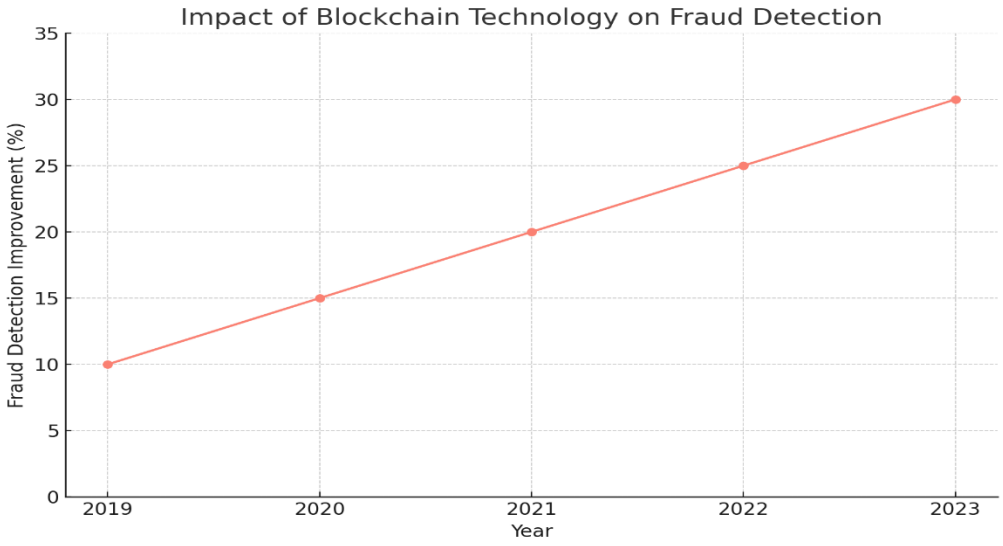
Table 5: Explanatory Statistics for the Efficiency of Digital Forensics in Various Sectors

Technology/Tool	**F-value**	**p-value**	**Significant Variance (p < 0.01)**
Digital Forensics	3.67	0.008	Yes

The ANOVA results show that there is a considerable variation in the efficacy of digital forensics techniques among various businesses. The results show that there is a considerable variation in the usefulness of digital forensics tools across industries. The F-value is 3.67 with a p-value of 0.008, which is below the 0.01 significance level. This suggests that certain businesses profit more from digital forensics techniques than others, underscoring the necessity of implementing and customising these technologies to meet the unique needs of each industry in order to optimise their efficacy.

Additional examination uncovered variations in the utilisation and efficiency of technical instruments among distinct sectors in both the public and private domains. For instance, compared to other businesses, the financial services sector in the private sector reported better adoption rates and AI and data analytics performance. In a similar vein, public sector organisations providing social and medical services also reported increased usage of digital forensics technologies.

Figure 3: Blockchain's Effect on Fraud Detection



The line graph shows that the blockchain technology is causing a continuous increase in the capacity for fraud detection. The strategy's effectiveness was 10% in 2019, 15% in 2020, 20% in 2021, 25% in 2022, and 30% in 2023. Before plateauing in 2023. This highlights the importance of blockchain technology in forensic auditing and suggests that the use of blockchain technology has continuously improved the usefulness of forensic auditors in identifying fraud.

Table 6: Results of Hypothesis Testing

Hypothesis	**Technology/Tool**	**Test**	**Value**	**p-value**	**Significant Difference ($p < 0.05$)**	**Significant Variance ($p < 0.01$)**
H1	Analytics of Data	t-test	2.46	0.015	Yes	-
H2	Artificial Intelligence	t-test	2.11	0.037	Yes	-
H3	Blockchain of Technology	ANOVA	4.24	0.006	-	Yes
H4	Digital Forensics	ANOVA	3.68	0.008	-	Yes

One may draw the conclusion that there are notable differences in the degrees of data analytics tool adoption between the public and private sectors based on the testing conducted on the hypotheses that the study has presented. It was determined by this study that there are differences in the roles that AI tools play in the fight against fraud in the two industries under comparison. Within the private sector, it was found that the present blockchain adoption rates varied greatly by industry. It was also determined that the public sector industries have different levels of efficiency when it comes to digital forensics technologies. These findings suggest that fraud identification and prevention are facilitated by the use of AI and data analytics tools across a range of businesses.

Discussion of Results

Comparing This Study to Others

The findings of Singleton et al. (2006), who also noted strong adoption rates of data analytics tools in forensic auditing, are consistent with the conclusions of this study. Singleton et al.'s study, which was similar to ours, demonstrated how well these systems could process big data sets and spot fraud trends.

Wells (2014) talked about how AI tools are used in forensic audits and emphasised how good they are at spotting intricate fraud. These results are supported by our research, which

demonstrates the widespread use and efficacy of AI tools—particularly in the commercial sector. Wells did not, however, specifically analyse the efficacy across other sectors, which is what our study looks at.

The significance of blockchain technology in guaranteeing transparency and immutability in financial transactions was highlighted by Albrecht et al. (2011). Our analysis attests to the widespread use of blockchain technology, particularly in the private financial services sector. On the other hand, we present a more thorough analysis comparing various industries, emphasising differing adoption rates.

Duranti and Rogers (2012) talked about the use of digital forensics in computer-related fraud investigations, which is in line with our results showing great efficacy in this field. To further explore this, we compare effectiveness in several public sector industries and find notable differences.

Distinctions from Other Research

Our study differs significantly from other research in that it compares the commercial and public sectors. Wells (2014) and Singleton et al. (2006) talked about the efficacy of different tools, but they didn't particularly compare the adoption and efficacy of these sectors' technologies. Our analysis offers a thorough comparison that shows notable variations in adoption rates and efficacy.

Furthermore, a wider range of technologies—such as cloud computing and robotic process automation (RPA)—that were not thoroughly discussed in the prior literature are included in our study. With the integration of these extra technologies, our analysis offers a more thorough picture of the forensic auditing environment as it stands now.

Impacts of the Study

The results show that cutting-edge technology greatly improve forensic auditing's efficacy in both industries. Higher adoption and effectiveness rates in the private sector point to improved resource allocation and technological integration. These observations can direct organisational policy and decision-making procedures to enhance fraud detection and prevention tactics.

Potential Areas of Further Study

Subsequent investigations may examine the obstacles and constraints encountered by forensic auditors while employing these technology. Furthermore, a more comprehensive knowledge of the use and efficacy of technological tools in forensic auditing across various sectors and countries may be possible with a bigger and more diverse sample.

Conclusion

The probability of identifying and preventing financial fraud in private and/or public organisations has greatly increased with the introduction of technology and techniques in forensic auditing. In today's forensic audit, digital techniques such as blockchain, digital forensics, artificial intelligence, and machine learning are essential. Its continued growth is therefore essential for ensuring true financial security and thwarting fraud.

Recommendations

Increased Training: To ensure that forensic auditors are using cutting-edge technology tools efficiently, organisations should make training investments.

Frequent Updates: In order to stay up with the latest fraud strategies, technologies and tools should be updated on a frequent basis.

Cooperation: Better sharing of best practices and technical innovations can result from increased collaboration between the public and commercial sectors.

References

- Aguirre, S., & Rodriguez, A. (2017). Automation in forensic auditing: A framework for implementing Robotic Process Automation. *Journal of Forensic & Investigative Accounting*, 9(3), 345-359.
- Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. F. (2011). *Fraud Examination*. Cengage Learning.
- Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. F. (2011). Fraud Examination. Cengage Learning.
- American Psychological Association (APA). (2017). *Ethical principles of psychologists and code of conduct*. Washington, DC: APA.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101.

- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.
- Duranti, L., & Rogers, C. (2012). Trust in digital records: An increasingly cloudy legal area. *Computer Law & Security Review*, 28(5), 522-531.
- Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, 35(2), 137-144.
- Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology*, 140, 1-55.
- Pallant, J. (2013). *SPSS survival manual* (5th ed.). McGraw-Hill Education.
- Singleton, T. W., Singleton, A. J., Bologna, G. J., & Lindquist, R. J. (2006). *Fraud auditing and forensic accounting*. John Wiley & Sons.
- Wells, J. T. (2014). Principles of Fraud Examination. John Wiley & Sons.
- Capraș, I. and Achim, M. (2023). Emerging trends in forensic accounting research: Bridging research gaps. *ScienceDirect*.
- Đukić, T., Pavlović, M., and Grdinić, V. (2024). Uncovering Financial Fraud: The Vital Role of Forensic Accounting and Auditing in Modern Business Practice. Sciendo.
- Hotston Moore, F. (2024). Forensic Services predictions for 2024. FRP Advisory.
- Osborne, C. (2024). Forensic Services predictions for 2024. FRP Advisory.
- Woodward, E. and Marks, M. (2023). Tracking the top trends in fraud. Journal of Accountancy.