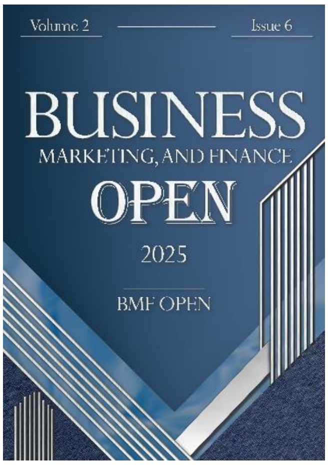
Presenting a Model for Fraud Prevention in the Public Sector Using Forensic Accounting

Ebrahim Nasiri[1], Khadijeh Eslami [2,*] and Khadijeh Rabiee [3]

[1] Department of Accounting, Ali.C., Islamic Azad University, Aliabad Katul, Iran;
[2] Department of Accounting, BG.C., Islamic Azad University, Bandargaz, Iran;
[3] Assistant Professor, Department of Accounting, Payam Noor University, Tehran, Iran;

* Correspondence: Kh.eslami@iau.ac.ir



Citation: Nasiri, E., Eslami, K., & Rabiee, K. (2025). Presenting a Model for Fraud Prevention in the Public Sector Using Forensic Accounting. *Business, Marketing, and Finance Open*, 2(6), 1-14.

Received: 19 March 2025
Revised: 17 May 2025
Accepted: 03 June 2025
Published: 01 November 2025

Abstract: The model for fraud prevention in the public sector using forensic accounting is designed based on the identification and analysis of weaknesses in existing financial and administrative processes. Enhancing transparency and accountability in financial and administrative reports can help reduce the risk of fraud. Additionally, the use of modern technologies such as big data and advanced analytics can assist in detecting suspicious patterns and abnormal behaviors. Ultimately, this model must be designed to align with the specific cultural, economic, and political characteristics of each country or public institution to effectively prevent fraud and enhance public trust. Therefore, this study was conducted with the aim of proposing a model for fraud prevention in the public sector through forensic accounting. The data required for Interpretive Structural Modeling (ISM) was gathered through interviews with 15 experts, specifically senior managers in the public sector who held at least a master's degree in accounting or auditing and had experience in forensic accounting (judiciary-appointed experts). In this research, a model was designed using ISM. The results of the ISM structural analysis, through the exploratory model, indicated that the dimensions of integrating forensic accounting and big data technology include digital evidence collection, collaboration with cybersecurity experts, a robust line of defense against fraud, and the development of appropriate structures and processes. Forensic accounting encompasses fraud detection and analysis, training and expertise, and cooperation with legal institutions. Big data technology includes dimensions such as identifying anomalous patterns, analyzing multi-source data, and enhancing information security.

Keywords: Public sector fraud, fraud prevention, forensic accounting.

1. Introduction

In recent decades, fraud in the public sector has emerged as one of the most pressing global governance challenges, threatening financial stability, public trust, and effective service delivery. While the scope and sophistication of fraud have grown in tandem with technological advancements and complex administrative systems, so too have the methods and models designed to prevent it. Within this context, forensic accounting has gained significant prominence as a proactive mechanism for addressing and mitigating financial misconduct in the public sphere. The integration of forensic accounting with emerging technologies such as artificial intelligence, big data analytics, and blockchain offers a new frontier for effective fraud detection and prevention strategies [1-3].

Fraud in public institutions is not merely a financial anomaly but a structural weakness that reflects deficiencies in accountability, oversight, and internal control mechanisms. Scholars argue that fraud in this sector is largely facilitated by the absence of a robust organizational culture, inadequate competency among financial personnel, and a disconnect between the roles of auditors and real-world anti-fraud outcomes [4, 5]. To combat this, comprehensive fraud prevention models must be designed with a multi-layered approach that includes forensic investigation, internal auditing, legal enforcement, and real-time monitoring systems [6, 7].

Forensic accounting, in particular, plays a critical role in fraud detection by not only identifying fraudulent activities but also by tracing financial misconduct through legally admissible documentation and evidence [8]. Its preventive function lies in increasing the perceived risk of detection among potential fraud perpetrators and reinforcing ethical standards within organizations [9]. As highlighted in the work of [10], identifying the risk factors influencing fraud, especially from the auditors' perspective, can serve as a foundational element for improving organizational resilience and performance.

However, the effectiveness of forensic accounting cannot be fully realized without the parallel development of technological capabilities. The rise of blockchain, artificial intelligence (AI), and data analytics has opened new pathways for fraud prediction and control. These tools not only automate anomaly detection but also enhance the traceability of transactions across vast and complex data networks [2, 11, 12]. For instance, the use of decision tree algorithms has been shown to significantly enhance the predictive accuracy of fraud detection systems in digital environments such as e-commerce and online banking [13]. Additionally, AI's ability to learn from historical fraud patterns enables dynamic adaptation to evolving fraud schemes, thus reducing both false positives and undetected fraud cases.

In line with these innovations, cybersecurity has emerged as a fundamental pillar in fraud prevention strategies, particularly in the financial services industry. Cybersecurity frameworks within fintech platforms are increasingly being designed to detect, prevent, and mitigate fraudulent activities before they impact institutional integrity [14]. Furthermore, the integration of fintech 3.5 systems enables real-time monitoring of digital financial transactions, reducing the window of opportunity for fraud to occur [15]. This convergence of digital security and financial oversight strengthens the foundation of forensic accounting by offering secure, immutable, and transparent platforms for tracking financial behavior.

Nevertheless, structural and institutional constraints continue to limit the full-scale implementation of fraud prevention models, especially in developing countries. In the Nigerian context, for instance, systemic corruption, limited audit capacity, and bureaucratic inertia have historically undermined anti-fraud initiatives [5, 16]. Studies reveal that despite the presence of statutory frameworks and financial management systems like the Government Integrated Financial Management Information System (GIFMIS), fraud continues to thrive due to poor enforcement and limited technological integration [7]. This underscores the need for a holistic model that not only emphasizes forensic accounting but also aligns with national governance capacities and institutional dynamics.

One of the key themes in recent literature is the importance of internal audit functions and auditor characteristics in curbing fraud. Research conducted in Pakistan suggests that the attributes of internal auditors—including their independence, technical expertise, and organizational commitment—are instrumental in reducing fraud risk and enhancing financial accountability [17]. Similarly, a study by [6] concluded that the integrity of auditors has a direct and positive relationship with the effectiveness of fraud prevention strategies. These findings reinforce the idea that the success of any forensic accounting model is inherently tied to the ethical and professional standards of the individuals tasked with its implementation.

A further critical factor in fraud prevention is the alignment of organizational culture with anti-fraud objectives. As highlighted by [4], the presence of a strong ethical culture, supported by transparent communication and accountability mechanisms, serves as a deterrent to fraudulent behavior. Conversely, environments that normalize or tolerate unethical practices tend to foster opportunities for fraud. This observation is consistent with findings from the public sector in Indonesia, where institutional culture was found to significantly influence the success of fraud prevention initiatives.

From a policy and implementation perspective, the effectiveness of fraud prevention models depends largely on multi-stakeholder engagement. According to [18], auditors must collaborate with regulatory bodies, law enforcement agencies, and IT professionals to build a comprehensive fraud defense system. This collaborative approach is essential for closing the audit expectation gap, especially in regions where public expectations exceed the practical scope of audit duties [16]. Moreover, the enforcement of financial reporting standards and legal sanctions against offenders creates a regulatory environment that discourages fraudulent practices and rewards compliance.

Fraud prevention models must also consider the implications of global financial systems, particularly in relation to cryptocurrencies and cross-border transactions. The decentralized nature of digital currencies presents unique challenges for fraud monitoring and enforcement, requiring the development of specialized forensic accounting techniques [3]. According to [19], fraudulent financial reporting often exploits regulatory gaps across jurisdictions, emphasizing the need for international cooperation and harmonized accounting practices.

Furthermore, fraud prevention strategies should be sensitive to the dynamic nature of fraud itself, which continually evolves in response to technological change, regulatory shifts, and market conditions. Therefore, fraud prevention frameworks must be iterative, data-driven, and flexible enough to adapt to new threats. As suggested by [20], the quality of financial reports in local governments improves significantly when fraud prevention mechanisms are designed with continuous feedback loops, risk assessments, and stakeholder involvement.

In conclusion, developing a robust fraud prevention model for the public sector necessitates a multi-disciplinary, technology-enabled, and context-sensitive approach. Forensic accounting serves as the cornerstone of such a model, offering investigative rigor, legal admissibility, and a deterrent effect. However, its success relies on complementary elements such as advanced technology, institutional integrity, auditor competence, organizational culture, and inter-agency collaboration. Therefore, this study aims to present a model for fraud prevention in the public sector using forensic accounting.

2. Methodology

In terms of its purpose, the present study is applied and exploratory in nature. The tools used in this research aim to formulate and present a model for fraud prevention in the public sector using forensic accounting. A mixed-methods approach was employed in the current research. Mixed-methods research combines quantitative and qualitative outputs within the framework of a single or multi-phase study. The fundamental principle of mixed-methods research is the utilization of both qualitative and quantitative techniques at different stages of the research, either simultaneously or sequentially, in a manner that their strengths are complementary and their weaknesses do not overlap. Furthermore, in terms of temporal sequence, qualitative data was collected first, followed by quantitative data. Subsequently, secondary interviews were conducted to confirm the findings. Therefore, the specific methodology used in this research is exploratory mixed-methods. Initially, qualitative data was collected through interviews with experts, and then quantitative data was gathered through questionnaires to follow up and complete the inquiry. Thus, both qualitative and quantitative methods were utilized in this study. First, components were extracted using qualitative methods, and then a conceptual model for the research was developed using Interpretive Structural Modeling (ISM).

The statistical population for the semi-structured expert interviews consisted of all senior managers in the public sector who held at least a master’s degree in accounting or auditing and had forensic accounting experience (as experts of the judiciary) and were familiar with theoretical data foundations. The sample was selected based on the total population and Morgan's table. The sampling method was simple random sampling from the accessible population. A total of 15 expert interviews were conducted in this research.

To conduct the Interpretive Structural Modeling (ISM), five main steps were undertaken:

Step 1: Formation of the Structural Self-Interaction Matrix (SSIM)

After identifying the underlying indicators of the phenomenon under study, an n×n square matrix of the existing indicators is designed. This matrix constitutes the ISM questionnaire. The Structural Self-Interaction Matrix (SSIM) is composed of the dimensions and indicators of the study, compared using four types of conceptual relationships. The SSIM is completed by experts and process-focused specialists. The collected data, based on the ISM modeling method, were summarized, and the final Structural Self-Interaction Matrix was formed. The logic of ISM is aligned with non-parametric methods and operates based on the mode of frequencies.

Step 2: Formation of the Reachability Matrix

The Reachability Matrix is derived by converting the SSIM into a binary matrix consisting of zeros and ones. To derive this matrix, in each row of the SSIM, the symbols X and V are replaced with one (1), and the symbols A and O are replaced with zero (0). The resulting matrix is referred to as the initial Reachability Matrix. The diagonal elements are set to one.

Step 3: Formation of the Final Reachability Matrix with Transitivity

After converting the matrix into a binary form, a secondary matrix must be designed to ensure transitive relationships are controlled. This means that if A leads to B and B leads to C, then A must also lead to C. If this transitive relationship is not represented, the matrix must be corrected to reflect it. Scientifically, this involves incorporating transitivity into the relationships among indicators to arrive at the final Reachability Matrix. This matrix is a square matrix where each cell contains a one (1) if there is reachability from one element to another through any number of steps; otherwise, it is zero (0).

Step 4: Determining Relationships and Hierarchical Leveling of Dimensions and Indicators

To determine the relationships and hierarchical levels of the criteria in the ISM model, the output set and the input set for each criterion must be derived from the Reachability Matrix.

- *Reachability Set (Outputs or Influenced Elements)*: Includes the criterion itself and the criteria it influences.
- *Antecedent Set (Inputs or Influencing Elements)*: Includes the criterion itself and the criteria that influence it.

After determining both sets, their intersection is computed. The first variable for which the intersection equals the reachability set (outputs) is considered the first-level indicator. These elements at the first level are those most influenced within the model. After identifying the first-level indicators, these elements are removed, and the process of calculating reachability and antecedent sets continues. This process is repeated until all indicators have been hierarchically categorized and removed.

Step 5: Driving Power–Dependence Diagram

In the ISM model, the mutual influences and interactions among criteria, as well as the relationships between different hierarchical levels, are clearly depicted, enhancing decision-making clarity for managers. To determine the key criteria, the driving power and dependence of each criterion are identified in the final Reachability Matrix.

This analysis is commonly referred to as MICMAC (Cross-Impact Matrix Multiplication Applied to Classification), although this naming is often misunderstood or misapplied.

3. Findings and Results

In this study, data analysis was conducted using the Content Validity Ratio (CVR), Interpretive Structural Modeling (ISM), and Structural Equation Modeling (SEM). These steps are explained in detail below.

At this stage, the CVR index was employed to determine the relative content validity of each factor. To achieve this, a questionnaire was distributed among experts, asking them to evaluate each factor and dimension based on a three-point Likert scale: "Essential", "Useful but not essential", and "Not necessary". Given that the number of experts was 15, if the CVR value of a factor exceeded 0.49, its content validity was considered confirmed. The results of applying the CVR index are presented in Table 1.

Table 1. CVR Value of Each Identified Factor

No.	Factors	CVR	Result	Dimensions	CVR	Result
1	Digital evidence collection	1	Accepted	Integration of forensic accounting and big data	1	Accepted
2	Cooperation with cybersecurity specialists	1	Accepted			
3	Cost reduction	0.46	Rejected			
4	Strong line of defense against fraud	1	Accepted			
5	Cultural promotion	0.2	Rejected			
6	Development of appropriate structures and processes	1	Accepted			
7	Fraud detection and analysis	1	Accepted	Role of forensic accounting	1	Accepted
8	Enhancing transparency	0.42	Rejected			
9	Accountability	0.2	Rejected			
10	Training and expertise	1	Accepted			
11	Risk analysis	0.46	Rejected			
12	Cooperation with legal institutions	1	Accepted			
13	Detection of abnormal patterns	1	Accepted	Role of big data technology	1	Accepted
14	Internal analysis	0.2	Rejected			
15	Multi-source data analysis	1	Accepted			
16	Information security enhancement	1	Accepted			
17	Fraud prevention through integration of forensic accounting and big data	1	Accepted	Public sector fraud prevention	1	Accepted
18	Fraud prevention using forensic accounting	1	Accepted			
19	Fraud prevention using big data technology	1	Accepted			

Table 2. CVR Values of Accepted Factors

No.	Factors	CVR	Result	Dimensions	CVR	Result
1	Digital evidence collection	1	Accepted	Integration of forensic accounting and big data	1	Accepted
2	Cooperation with cybersecurity specialists	1	Accepted			
3	Strong line of defense against fraud	1	Accepted			
4	Development of appropriate structures and processes	1	Accepted			
5	Fraud detection and analysis	1	Accepted	Role of forensic accounting	1	Accepted
6	Training and expertise	1	Accepted			
7	Cooperation with legal institutions	1	Accepted			
8	Detection of abnormal patterns	1	Accepted	Role of big data technology	1	Accepted
9	Multi-source data analysis	1	Accepted			
10	Information security enhancement	1	Accepted			

11	Fraud prevention through integration of forensic accounting and big data	1	Accepted	Public sector fraud prevention	1	Accepted
12	Fraud prevention using forensic accounting	1	Accepted			
13	Fraud prevention using big data technology	1	Accepted			

As indicated in the above table, 13 factors across 4 dimensions were confirmed by the experts. Therefore, these 13 factors were utilized for the purpose of "developing a model for fraud prevention in the public sector using forensic accounting."

Step One: Identifying Factors Related to the Issue

The selection method of the factors has been fully explained. Therefore, these 13 factors are utilized for model development.

Step Two: Formation of the Structural Self-Interaction Matrix

After determining the factors, the ISM questionnaire was designed. Experts evaluated the factors in pairs and determined their relationships using the following symbols:

- **V**: if factor *i* influences factor *j*
- **A**: if factor *j* influences factor *i*
- **X**: if there is mutual influence between factors *i* and *j*
- **O**: if there is no relationship between factors *i* and *j*

The results from the expert questionnaires for the evaluated factors are presented in Table 3.

Table 3. Results from the Expert Questionnaires

No.	Factors	1	2	3	4	5	6	7	8	9	10	11	12	13
1	Digital evidence collection	—	O	O	O	O	O	O	O	O	O	V	V	V
2	Cooperation with cybersecurity specialists		—	O	O	O	O	O	O	O	O	V	V	V
3	Strong line of defense against fraud			—	O	O	O	O	O	O	O	V	V	V
4	Development of appropriate structures and processes				—	O	O	O	O	O	O	V	V	V
5	Fraud detection and analysis					—	O	O	O	O	O	V	V	V
6	Training and expertise						—	O	O	O	O	V	V	V
7	Cooperation with legal institutions							—	O	O	O	V	V	V
8	Detection of abnormal patterns								—	O	O	V	V	V
9	Multi-source data analysis									—	V	V	V	V
10	Enhancing information security										—	V	V	V
11	Fraud prevention via integration of forensic accounting and big data											—	O	O
12	Fraud prevention via forensic accounting												—	O
13	Fraud prevention via big data technology													—

Step Three: Formation of the Initial Reachability Matrix

The initial reachability matrix is obtained by converting the Structural Self-Interaction Matrix into a binary matrix (0s and 1s). The conversion is based on the following rules:

1. If the entry (i, j) in the SSIM is symbol **V**, then in the initial reachability matrix (i, j) is 1 and (j, i) is 0.
2. If the entry (i, j) is **A**, then (i, j) is 0 and (j, i) is 1.
3. If the entry is **X**, then both (i, j) and (j, i) are 1.
4. If the entry is **O**, then both (i, j) and (j, i) are 0.

Table 4. Initial Reachability Matrix

No.	Factors	1	2	3	4	5	6	7	8	9	10	11	12	13
1	Digital evidence collection	1	0	0	0	0	0	0	0	0	0	1	1	1
2	Cooperation with cybersecurity specialists	0	1	0	0	0	0	0	0	0	0	1	1	1
3	Strong line of defense against fraud	0	0	1	0	0	0	0	0	0	0	1	1	1
4	Development of appropriate structures and processes	0	0	0	1	0	0	0	0	0	0	1	1	1
5	Fraud detection and analysis	0	0	0	0	1	0	0	0	0	0	1	1	1
6	Training and expertise	0	0	0	0	0	1	0	0	0	0	1	1	1
7	Cooperation with legal institutions	0	0	0	0	0	0	1	0	0	0	1	1	1
8	Detection of abnormal patterns	0	0	0	0	0	0	0	1	0	0	1	1	1
9	Multi-source data analysis	0	0	0	0	0	0	0	0	1	0	1	1	1
10	Enhancing information security	0	0	0	0	0	0	0	0	0	1	1	1	1
11	Fraud prevention via integration of forensic accounting and big data	0	0	0	0	0	0	0	0	0	0	1	0	0
12	Fraud prevention via forensic accounting	0	0	0	0	0	0	0	0	0	0	0	1	0
13	Fraud prevention via big data technology	0	0	0	0	0	0							

Step Four: Formation of the Final Reachability Matrix

Once the initial reachability matrix is established, secondary (transitive) relationships between factors are checked. A transitive relationship implies that if factor *i* leads to factor *j*, and *j* leads to factor *k*, then *i* should also lead to *k*. If such transitive links are absent in the initial matrix, they must be added. This adjustment process is referred to as "reconciliation" of the initial reachability matrix.

In this step, all secondary relationships between the factors were examined. However, no additional transitive relations were identified. Therefore, the final reachability matrix remained identical to the initial matrix.

This matrix also displays each factor's driving power (the number of factors it influences, including itself) and dependence (the number of factors that influence it, including itself).

Table 5. Final Reachability Matrix

No.	Factors	1	2	3	4	5	6	7	8	9	10	11	12	13	Driving Power
1	Digital evidence collection	1	0	0	0	0	0	0	0	0	0	1	1	1	4
2	Cooperation with cybersecurity specialists	0	1	0	0	0	0	0	0	0	0	1	1	1	4
3	Strong line of defense against fraud	0	0	1	0	0	0	0	0	0	0	1	1	1	4
4	Development of appropriate structures and processes	0	0	0	1	0	0	0	0	0	0	1	1	1	4
5	Fraud detection and analysis	0	0	0	0	1	0	0	0	0	0	1	1	1	4
6	Training and expertise	0	0	0	0	0	1	0	0	0	0	1	1	1	4
7	Cooperation with legal institutions	0	0	0	0	0	0	1	0	0	0	1	1	1	4
8	Detection of abnormal patterns	0	0	0	0	0	0	0	1	0	0	1	1	1	4
9	Multi-source data analysis	0	0	0	0	0	0	0	0	1	0	1	1	1	4
10	Enhancing information security	0	0	0	0	0	0	0	0	0	1	1	1	1	4
11	Fraud prevention via integration of forensic accounting and big data	0	0	0	0	0	0	0	0	0	0	1	0	0	1
12	Fraud prevention via forensic accounting	0	0	0	0	0	0	0	0	0	0	0	1	0	1
13	Fraud prevention via big data technology	0	0	0	0	0	0	0	0	0	0	0	0	1	1
	Dependence	1	1	1	1	1	1	1	1	1	1	11	11	11	—

As shown, each of the first 10 factors has a high degree of influence and interconnectedness with the final fraud prevention indicators (factors 11–13), which have high levels of dependence. This confirms the structural role of these core operational factors in enabling integrated fraud prevention strategies.

As shown in the table above, the output sets of Factors 11, 12, and 13 are identical. Therefore, these factors are categorized as dependent factors at Level One. Consequently, to proceed with further hierarchical structuring, these factors must be removed from the table. The following table presents the second iteration of the level partitioning process.

Table 6. Level Structuring (Second Iteration)

Row	Factors	Output Set	Input Set	Common Set	Level
1	Digital evidence collection	1	1	1	2
2	Cooperation with cybersecurity specialists	2	2	2	2
3	Strong line of defense against fraud	3	3	3	2
4	Development of appropriate structures/processes	4	4	4	2
5	Fraud detection and analysis	5	5	5	2
6	Training and expertise	6	6	6	2
7	Cooperation with legal institutions	7	7	7	2
8	Detection of abnormal patterns	8	8	8	2
9	Multi-source data analysis	9	9	9	2
10	Enhancing information security	10	10	10	2

As illustrated in the table above, the output sets of Factors 1 through 10 are identical. Accordingly, these factors are categorized as influencing factors at Level Two. Therefore, to complete the level structuring process, these factors are also removed from the table. As a result, the level structuring process is concluded.

Step Six: Drawing the Final Model

At this stage, based on the factor levels and the final reachability matrix, an initial model is constructed. After eliminating transitive links from the initial model, the final ISM model is developed. Accordingly, the ISM model derived from the influencing factors in the forensic accounting framework, embedded in big data technology for public sector fraud prevention in Iran, is illustrated in Figure 1.

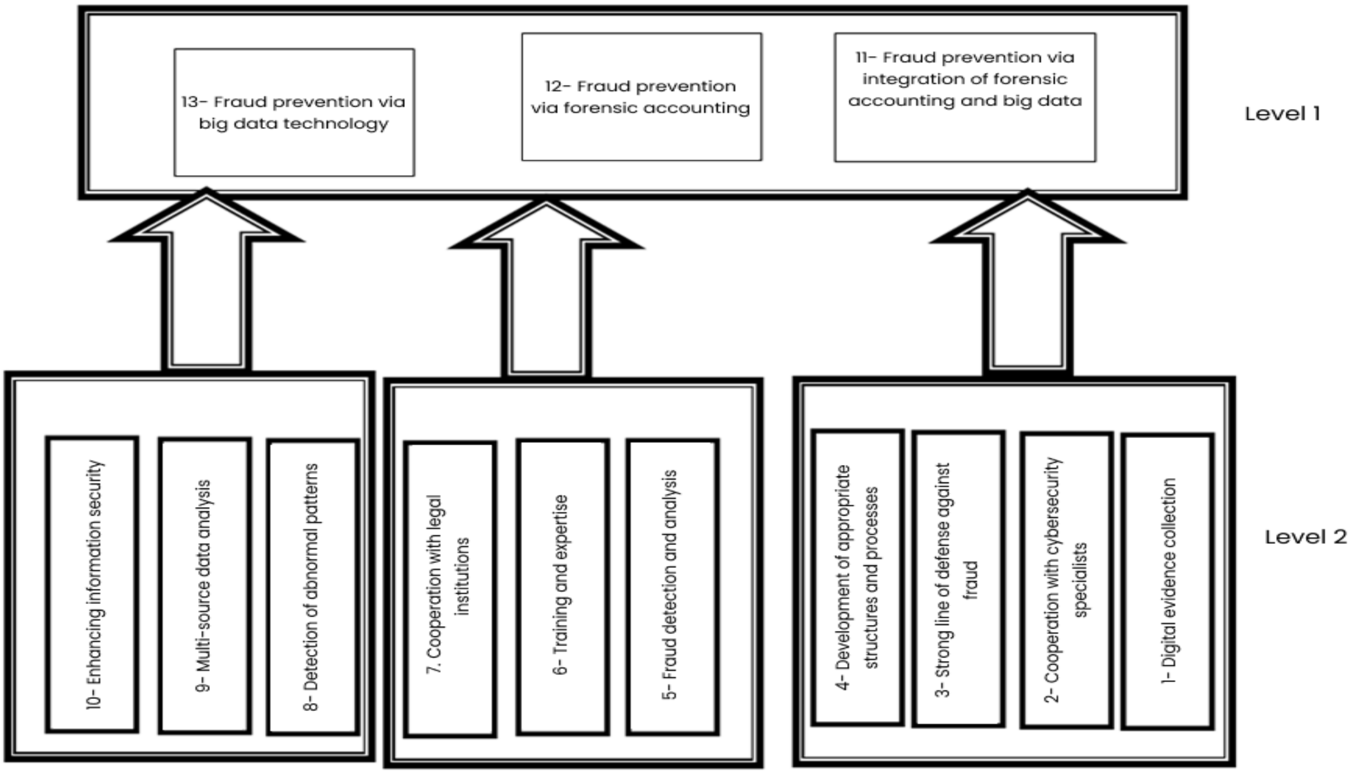

13- Fraud prevention via big data technology
12- Fraud prevention via forensic accounting
11- Fraud prevention via integration of forensic accounting and big data
Level 1
10- Enhancing information security
9- Multi-source data analysis
8- Detection of abnormal patterns
7. Cooperation with legal institutions
6- Training and expertise
5- Fraud detection and analysis
4- Development of appropriate structures and processes
3- Strong line of defense against fraud
2- Cooperation with cybersecurity specialists
1- Digital evidence collection
Level 2

Figure 1: Initial ISM Model

As depicted in the figure above, Factors 11, 12, and 13 are located at Level One. These are the most dependent factors in the model. Additionally, Factors 1 through 10 are placed at Level Two, representing the most influential factors in the model. Based on the classification of these factors, the final ISM model is represented in Figure 2.

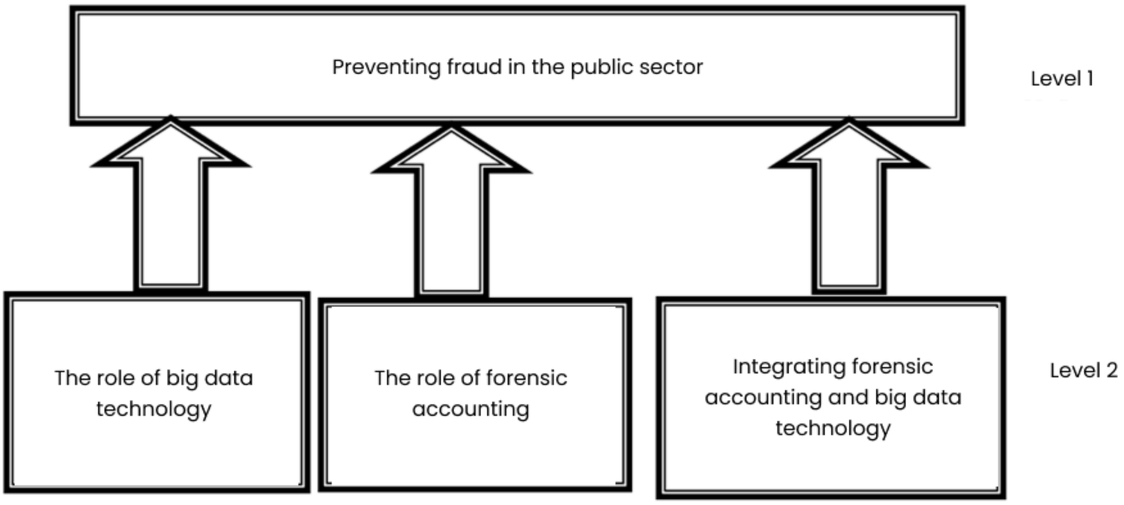

Preventing fraud in the public sector
Level 1
The role of big data technology
The role of forensic accounting
Integrating forensic accounting and big data technology
Level 2

Figure 2: Final ISM Model

Step Seven: Driving Power–Dependence Analysis (MICMAC Diagram)

At this stage, the factors are categorized into four groups. The first group consists of autonomous factors (Quadrant I) that have both low driving power and low dependence. These factors are relatively detached from other elements and exhibit minimal interactions.

The second group includes dependent factors (Quadrant II), which have low driving power but high dependence. The third group consists of linkage factors (Quadrant III). These elements possess both high driving power and high dependence, meaning that any change in these factors will significantly influence and be influenced by other factors. The fourth group comprises independent factors (Quadrant IV) with high driving power and low dependence. Factors with high driving power are often referred to as key factors. It is evident that such elements fall into either the independent or linkage categories.

By summing the "1" entries in each row and column of the final reachability matrix, the driving power and dependence level of each factor are calculated. Based on this, the driving power–dependence diagram is plotted.

Using the data obtained from Step Four, the studied factors can be categorized into four levels based on their driving power (influence over other factors) and dependence (degree of being influenced by other factors):

- **Autonomous Factors**: These are factors with minimal dependence on and minimal influence over other factors.
- **Dependent Factors**: These are factors that exhibit high dependence on other factors.
- **Linkage (Connected) Factors**: These are factors with bidirectional relationships with other factors.
- **Independent (Driving) Factors**: These are factors that exert significant influence over other factors.

To determine the position of each factor in the MICMAC matrix, their driving power and dependence values are used. These values are derived from the final reachability matrix. Table 7 presents the driving power and dependence of each factor.

Table 7. Driving Power and Dependence of Each Factor

No.	Factor	Dependence	Driving Power
1	Digital evidence collection	1	4
2	Cooperation with cybersecurity specialists	1	4
3	Strong line of defense against fraud	1	4
4	Development of appropriate structures and processes	1	4
5	Fraud detection and analysis	1	4
6	Training and expertise	1	4
7	Cooperation with legal institutions	1	4
8	Detection of abnormal patterns	1	4
9	Multi-source data analysis	1	4
10	Enhancing information security	1	4
11	Fraud prevention via integration of forensic accounting and big data	11	1
12	Fraud prevention via forensic accounting	11	1
13	Fraud prevention via big data technology	11	1

Based on the coordinates of the factors provided in the table above, the MICMAC matrix is constructed (Figure 3).

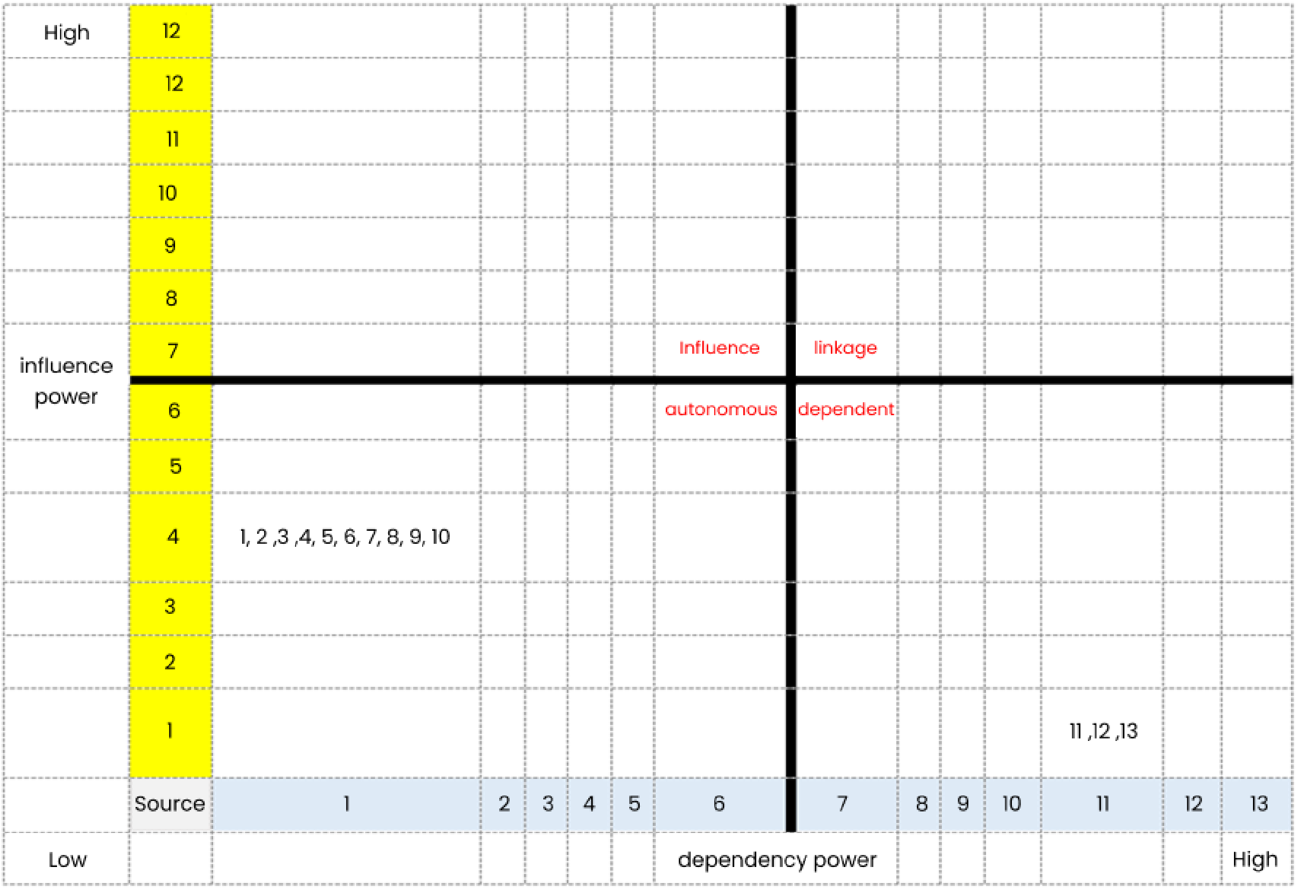


Figure 3. MICMAC Matrix

As shown in the above figure (MICMAC matrix), factors 1 through 10 fall into the Autonomous Zone. These factors possess low dependence and low driving power. Factors 11, 12, and 13 fall into the Dependent Zone. These factors exhibit low driving power but high dependence on other factors.

At this point, the Interpretive Structural Modeling (ISM) process concludes.

4. Discussion and Conclusion

The findings of this study, which aimed to develop a fraud prevention model for the public sector through the integration of forensic accounting and emerging technologies, underscore the critical role of multifactorial dimensions—ranging from digital evidence collection to cybersecurity collaboration—in shaping an effective anti-fraud infrastructure. The model's structure, validated through Interpretive Structural Modeling (ISM), revealed that ten operational factors (e.g., training and expertise, collaboration with legal institutions, multi-source data analysis) exert strong driving power while three outcome-level components (fraud prevention through forensic accounting, big data, and their integration) were highly dependent. This hierarchy indicates that fraud prevention in the public sector hinges upon upstream institutional and technical capacities that feed into overarching strategic outcomes.

The significant influence of factors such as "digital evidence collection" and "cooperation with cybersecurity experts" aligns with the growing consensus on the transformative role of technology in combating financial irregularities. This is consistent with the assertions of [2], who emphasized the potential of AI-driven systems to predict, detect, and prevent fraudulent transactions in real-time. Moreover, the integration of forensic accounting with big data analytics, as validated in this study, complements the work of [11] and [13], who found that digital ledger technologies and decision tree algorithms significantly enhance fraud detection capabilities in high-volume data environments. These technologies not only reduce the operational burden on auditors but also increase the transparency and auditability of financial records.

The high validity scores (CVR = 1.00) across all 13 selected components, especially for "fraud detection and analysis," "training and expertise," and "information security," further highlight the necessity of both human capital and system security in public financial oversight. As suggested by [17], the internal audit function is most effective when supported by skilled professionals who can interpret red flags and implement evidence-based controls. Similarly, [6] demonstrated that auditor integrity and commitment are pivotal in preventing fraud, reinforcing our model's inclusion of capacity-building and training as critical driving factors.

Interestingly, the model's identification of three highly dependent elements—fraud prevention through forensic accounting, big data technology, and their integration—reflects the layered and outcome-oriented nature of anti-fraud strategies. These findings are congruent with [1], who argued that forensic accounting acts as a reactive and preventive tool only when embedded within a broader digital and institutional architecture. Moreover, [19] highlighted how fraudulent reporting in public institutions often stems from the absence of such an integrated framework. The present study adds empirical support to this viewpoint by demonstrating how operational components (e.g., cybersecurity, evidence collection) form the infrastructure upon which systemic prevention mechanisms rest.

The MICMAC analysis further revealed that all driving factors fell into the "autonomous" quadrant—indicating high influence and low dependence—whereas the outcome elements were categorized as "dependent," with low driving power but high reliance on other variables. This structure suggests a clear causal pathway in which effective implementation of foundational strategies triggers downstream anti-fraud outcomes. It resonates with the findings of [4], who emphasized that the role of organizational culture, employee competence, and internal audit must precede any effective prevention strategy. Similarly, [20] identified a strong link between quality financial reporting in local governments and the implementation of such foundational capacities.

The inclusion of cybersecurity collaboration and data integrity protection within the model responds to calls from the literature to prioritize digital security in public sector financial operations. [14] underscored how fintech-enabled fraud detection systems benefit from robust cybersecurity architectures that detect threats before they escalate. This finding is echoed in [15], who demonstrated that reducing opportunity and access is just as critical as improving detection mechanisms. Therefore, the current model's emphasis on proactive safeguards supports the shift toward preventive, rather than solely reactive, approaches to fraud management.

Moreover, the study's results align with the theoretical framework proposed by [18], who argued that auditors, regulators, and law enforcement must operate in an integrated system to ensure the effectiveness of fraud prevention. This inter-agency collaboration model is indirectly reflected in our findings, where components such as "cooperation with legal institutions" and "interdisciplinary data analytics" form the connective tissue between operational controls and broader institutional effectiveness. This alignment lends external validity to the current study and supports its applicability beyond the Nigerian context.

Another notable contribution of this study is its validation of digital tools in environments traditionally governed by manual oversight and legacy systems. For instance, the strong role of "multi-source data analysis" and "pattern detection" validates earlier claims by [12] that hybrid fraud detection systems—combining transaction history, behavioral analytics, and machine learning—significantly improve the accuracy and timeliness of fraud detection. Additionally, [3] cautioned that the lack of control mechanisms in cryptocurrency environments facilitates money laundering and fraud. The inclusion of secure data analysis techniques in this study's model offers a pathway to counteract such vulnerabilities.

At the conceptual level, this study complements the theoretical contributions of [8], who emphasized the dual role of forensic accounting in both prevention and post-fraud litigation. By demonstrating how forensic accounting's utility increases when embedded within a digital and procedural framework, our findings suggest a need to transition from isolated forensic interventions to system-integrated prevention architectures. This evolution supports the broader trend in fraud studies toward systematization and cross-functional governance.

In sum, the validated model offers a structured and actionable framework that integrates institutional, technological, and professional components for the prevention of fraud in the public sector. It reflects the best practices identified in the literature while also offering new insights into how operational elements cascade into systemic outcomes. The study not only reinforces established knowledge but also bridges theoretical gaps by emphasizing the relational hierarchy among anti-fraud strategies.

Despite the comprehensive nature of this study, several limitations should be acknowledged. First, the research was conducted using a relatively small sample of 15 public sector experts, which may limit the generalizability of the model across broader institutional or international contexts. Second, the reliance on expert judgment for ISM modeling, while methodologically appropriate, introduces subjectivity that could affect the robustness of the hierarchical relationships established. Third, the study focused predominantly on structural and technical aspects, potentially overlooking softer behavioral or psychological variables that influence fraud dynamics, such as whistleblower culture or employee morale.

Future research could expand the model by incorporating a larger and more diverse sample from different governmental and non-governmental institutions to enhance generalizability. Researchers may also employ confirmatory statistical techniques such as Structural Equation Modeling (SEM) on larger datasets to validate and refine the relational strength of the proposed variables. Moreover, future studies could explore the behavioral and organizational psychology dimensions of fraud, focusing on motivations, deterrence mechanisms, and the role of ethics training. Cross-national comparative studies would also be valuable in understanding how cultural and regulatory differences impact the effectiveness of fraud prevention frameworks.

Practitioners should prioritize the development of internal capacities, especially in the areas of training, digital evidence collection, and cybersecurity. Governments and public agencies must invest in integrated information systems that enable real-time data analysis, fraud pattern recognition, and automated alerts. A multidisciplinary approach involving auditors, IT professionals, and legal experts should be institutionalized for sustained fraud monitoring. Additionally, public sector leadership should promote an ethical organizational culture through clear policies, accountability frameworks, and incentivized compliance to foster long-term fraud resilience.

Authors' Contributions

Authors equally contributed to this article.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

[1] S. Abdulrahman, "Forensic accounting and fraud prevention in Nigerian public sector: A conceptual paper," *International Journal of Accounting & Finance Review,* vol. 4, no. 2, pp. 13-21, 2019, doi: 10.46281/ijafr.v4i2.389.

[2] O. Odeyemi, "Reviewing the Role of AI in Fraud Detection and Prevention in Financial Services," *International Journal of Science and Research Archive,* vol. 11, no. 1, pp. 2101-2110, 2024, doi: 10.30574/ijsra.2024.11.1.0279.

[3] Z. Izadi and N. Arzaniyan, "Preventing money laundering and fraud in the context of global cryptocurrency usage," *Journal of Crime Prevention Approaches,* vol. 2, no. 1, pp. 37-56, 2019.

[4] D. A. Nugroho, R. Sari, and C. Kuntadi, "Factors Affecting Fraud Prevention: Organizational Culture, Human Resource Competence and the Role of The Internal Auditor," *Dinasti International Journal of Education Management and Social Science,* vol. 4, no. 4, pp. 627-636, 2023.

[5] R. Abdullahi and N. Mansor, "Fraud prevention initiatives in the Nigerian public sector," *Journal of Financial Crime,* vol. 25, no. 2, pp. 527-544, 2018, doi: 10.1108/JFC-02-2015-0008.

[6] M. H. Rifai and A. W. Mardijuwono, "Relationship between auditor integrity and organizational commitment to fraud prevention," *Asian Journal of Accounting Research,* vol. 5, no. 2, pp. 315-325, 2020, doi: 10.1108/AJAR-02-2020-0011.

[7] O. S. Ajao, O. O. Aremu, and I. J. Ufuoma, "Government Integrated Financial Management Information System and Fraud Prevention in Nigeria," *Journal of Finance and Accounting,* vol. 10, no. 3, pp. 151-159, 2022, doi: 10.11648/j.jfa.20221003.11.

[8] J. Barzegari and S. Sehat, "Forensic Accounting and Fraud Prevention (A Review of Studies and Theoretical Discussions)," in *Fourth International Conference on Applied Research in Management and Accounting*, Tehran, 2016: Shahid Beheshti University.

[9] L. Zager, S. S. Malis, and A. Novak, "The Role and Responsibility of Auditors in Prevention and Detection of Fraudulent Financial Reporting," *Procedia Economics and Finance,* vol. 39, pp. 693-700, 2016/01/01/ 2016, doi: 10.1016/S2212-5671(16)30291-X.

[10] J. Moradi, R. Rostami, and R. Zare, "Recognizing Risk Factors Affecting Fraud Probability in Financial Reporting from Auditors' Viewpoint and Its Impact on Firms' Performance," *Journal of Accounting Advances,* vol. 6, no. 1, pp. 141-173, 2014, doi: 10.22099/jaa.2014.2261.

[11] E. M. S. W. Balagolla, W. P. C. Fernando, and R. M. N. S. Rathnayake, "Credit Card Fraud Prevention Using Blockchain," 2021, doi: 10.1109/I2CT51068.2021.9418192.

[12] V. Kansal, "Analysis and Design of Fraud Detection and Prevention Techniques in Card Based Financial," pp. 1020-1023, 2023, doi: 10.13052/rp-9788770040723.194.

[13] P. K. R. Hole, "Fraud Detection and Prevention in E-Commerce Using Decision Tree Algorithm," *International Journal for Research in Applied Science and Engineering Technology,* vol. 12, no. 4, pp. 2187-2196, 2024, doi: 10.22214/ijraset.2024.60307.

[14] N. Selvaraj, "The essence of cybersecurity through fintech 3.5 in preventing and detecting financial fraud: a literature review," *Electronic Journal of Business and Management,* vol. 6, no. 2, pp. 18-29, 2021.

[15] J. B. Suh, R. Nicolaides, and R. Trafford, "The effects of reducing opportunity and fraud risk factors on the occurrence of occupational fraud in financial institutions," *International Journal of Law, Crime and Justice,* vol. 56, pp. 79-88, 2019/03/01/ 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1756061618302180.

[16] S. Sule, N. Z. M. Yusof, and K. M. K. Bahador, "Users' Perceptions on Auditors' Responsibilities for Fraud Prevention, Detection and Audit Expectation GAP in Nigeria," *Asian Journal of Economics, Business and Accounting,* pp. 1-10, 2019, doi: 10.9734/AJEBA/2019/46832.

[17] N. Khan, A. Rafay, and A. Shakeel, "Attributes of Internal Audit and Prevention, Detection and Assessment of Fraud in Pakistan," *The Lahore Journal of Business,* vol. 9, no. 1, pp. 33-58, 2020, doi: 10.35536/ljb.2020.v9.i1.a2.

[18] S. S. Halbouni, "The role of auditors in preventing, detecting, and reporting fraud: The case of the U nited A rab E mirates (UAE)," *International Journal of Auditing,* vol. 19, no. 2, pp. 117-130, 2015, doi: 10.1111/ijau.12040.

[19] S. Milojević, S. Knezevic, and V. Šebek, "Identification and prevention of fraudulent financial reporting," *Tokovi osiguranja,* vol. 40, pp. 146-182, 2024, doi: 10.5937/TokOsig2401146M.

[20] H. Umar, A. Indriani, and R. B. Purba, "The Determinant Fraud Prevention of Quality Local Government's Financial Report," *Jurnal Akuntansi Dan Bisnis Jurnal Program Studi Akuntansi,* vol. 5, no. 1, p. 41, 2019, doi: 10.31289/jab.v5i1.2310.