Selection of a Trustworthy Technique for Fraud Prevention in the Digital Banking Sector

Bandar Ali M. Al-Rami Al-Ghamdi
Faculty of Computer Studies, Arab Open University, Riyadh 11681, Saudi Arabia

***Abstract*—Digital banking fraud poses a threat to the global economy and fintech applications. Sustainable models are essential to address this issue and minimize its economic impact. Hybrid methods have been developed to assess strategies for preventing digital banking fraud, aiding global stakeholders in making well-informed judgments. However, many of these models concentrate on the numerical features of digital banking ratios while overlooking crucial financial fraud protection qualities. This paper introduces a computational method for discovering and measuring the influence of digital banking fraud prevention strategies on sustainable fraud prevention. This innovative approach combines intuitionistic fuzzy set theory and the analytical network process for decision-making. Initially, an intuitionistic fuzzy expert system prioritizes crucial indices based on the preferences of financial decision-makers. This technique is then compared to alternative decision-making models across multiple variables. Empirical data demonstrate the superiority of the intuitionistic fuzzy-based decision-making system, outperforming other models and facilitating the recognition of financial statement fraud in global banking networks. Consequently, it offers a sustainable fintech solution. The findings of this study are pertinent to fintech scholars and practitioners engaged in the global battle against digital banking fraud.**

***Keywords*—Digital banking fraud; analytical network process; intuitionistic fuzzy sets; fraud prevention and detection**

I. Introduction

Fraudsters in Saudi Arabia have rapidly adapted to modern technological systems, leaving old brick-and-mortar institutions behind [1–2]. Criminal techniques are constantly evolving, posing a threat to the entire payment ecosystem and prompting regulatory attention across all banks, regardless of their level of digital transformation [3–4].

The adoption of online banking in Saudi Arabia is expected to rise by 16.7% from 2024 to 2028 [5], indicating significant growth in KSA's digital banking. After fifteen years of continuous growth, the online banking rate is predicted to peak at 68.16 percent in 2028. It is noteworthy that Saudi Arabia has consistently increased internet banking penetration in recent years, demonstrating a persistent trend of people using digital banking services for financial interaction and management.

The growing digitization of global banking has necessitated an evaluation of hybrid decision-making (DM) methods to combat digital banking fraud [6–8]. Digital banking fraud encompasses phishing, spoofing, identity theft, account fraud, and transaction fraud. Phishing and spoofing, involving unwary recipients receiving misleading emails, phone calls, and texts from seemingly reputable sources, are common occurrences [9–10]. These attempts aim to steal sensitive data or gain access to computer networks, resulting in financial losses and identity theft.

Given the severity of these frauds, Saudi business boards must implement stronger and more effective fraud prevention measures. Fraud detection and mitigation are not only cost-effective but also essential for reputation protection. Saudi Arabian specialists use multiple characteristic decision-making (MCDM) methods to evaluate digital banking fraud prevention technologies [5–7]. The Analytical Network Process (ANP) serves as a suitable model for comparing characteristics to solutions. However, due to decision-makers' subjectivity and uncertainties in input data, a more realistic strategy that effectively addresses these uncertainties is needed.

The intuitionistic fuzzy ANP emerges as a better and more realistic method for evaluating alternative solutions to Saudi Arabia's digital banking fraud problem. It assists decision-makers in choosing actions that align with goals by considering user expertise and historical perspectives on the issue. By incorporating the views of Saudi Arabian subject-matter experts, the intuitionistic fuzzy-ANP model addresses local fintech differences effectively.

This research enhances the evaluation of fraud prevention models in the financial accounts of Saudi Arabian fintech applications using the intuitive fuzzy-ANP methodology. The study has two objectives: first, to understand the drivers of Saudi fintech apps and digital banking fraud, and second, to assess how well the intuitionistic fuzzy-ANP utilizes these characteristics to prevent wrongdoing. The study recommends a systematic and integrated approach to investigation and prevention to identify abnormalities and conduct comprehensive fraud assessments [8–12]. These early investigations lay the groundwork for further analyses and in-depth inquiries to resolve the issue.

This article analyzes past trends and statistics to provide readers with a brief introduction to fraud analysis and prevention in fintech apps. The next section is a literature overview of pertinent studies by earlier researchers. The final section discusses features used to evaluate digital banking fraud models and suggests a hierarchical architecture for Saudi Arabian fraud detection and prevention. The study employs intuitionistic fuzzy-ANP to numerically deconstruct the hierarchical problem. The discussion will include a comparative study after presenting the findings. The paper concludes with a summary of the complex discussion and outlines study limitations.

II. PREVENTING DIGITAL BANKING FRAUDS

Saudi Arabia needs a comprehensive digital banking fraud prevention strategy to guide managers and key departments in recognizing, assessing, and responding to possible fraud [13-15]. This well-developed strategy details each organization's function and its duties. Its success depends on senior management's active participation in its formulation. Effective communication between decision-makers, managers, law enforcement agencies, customers, and external organizations helps develop robust risk analysis, prediction, and DM procedures and fosters seamless collaboration.

Comprehensive training for the entire team is necessary to accurately apply the policy and handle situations in accordance with the fraud prevention strategy [16-17]. Before preventing fraud, this training is required. To ensure efficacy, the fraud prevention plan should be thoroughly examined, rehearsed, and checked for flaws. This rigorous preparation is necessary since the fraud prevention plan executes activities and ensures fraud detection and prevention. The organization's nature, size, and operating environment have all played a significant role in shaping the Saudi strategy.

Before establishing the best decision support tools, Saudi Arabia needs a well-defined network to manage its many fraud prevention techniques. Fraud in digital banking applications is diverse; thus, decision support systems should be tailored to the individual difficulties [5-6]. The following paragraph examines the fundamental principles of a proactive preventative strategy and its components. The following paragraph elaborates on this strong discussion and analysis.

A. Fraud Prevention Planning

Upper management's active involvement across all business units and their unwavering support underpin the plan's concepts in Saudi Arabia [15]. It has four main steps, as explained below. After refining with Saudi-specific examples, the process was reduced to four parts. The organization's management, fraud risk assessment, views of fraud detection, and a complete fraud prevention policy for stakeholders are covered in these phases. Each phase is interdependent, and sub-processes are carefully structured to match. The hierarchical design in Fig. 1 shows how to build a fraud prevention plan model. Organizational management subprocesses include management attitude, integrity, policy commitment, and strict enforcement. Below is a full description of each subprocess:

1) Organization's management: Any fraud prevention plan begins with a thorough management structure review. Senior management must be involved in organisational units while developing a fraud prevention strategy. This involvement should be regular to be effective. The top of the firm oversees all plan execution processes as a protective cover. This level includes management's thinking, unshakable dedication to integrity policies, and rigorous implementation. Fig. 1 shows the complex interaction of these mechanisms [4–5].

2) Fraud risk assessment: Any comprehensive fraud protection plan's second crucial step is a thorough analysis of digital banking fraud risk. This phase assesses the like-lihood of illegal activity. It involves creating specialised teams, mitigating risks, and monitoring and controlling the strategy. This step includes the creation of the risk as-sessment team, the creation of a rigorous risk assessment methodology, and the im-plementation of compliance monitoring measures [9–12]. Fig. 1 shows the fraud risk assessment procedure in steps.

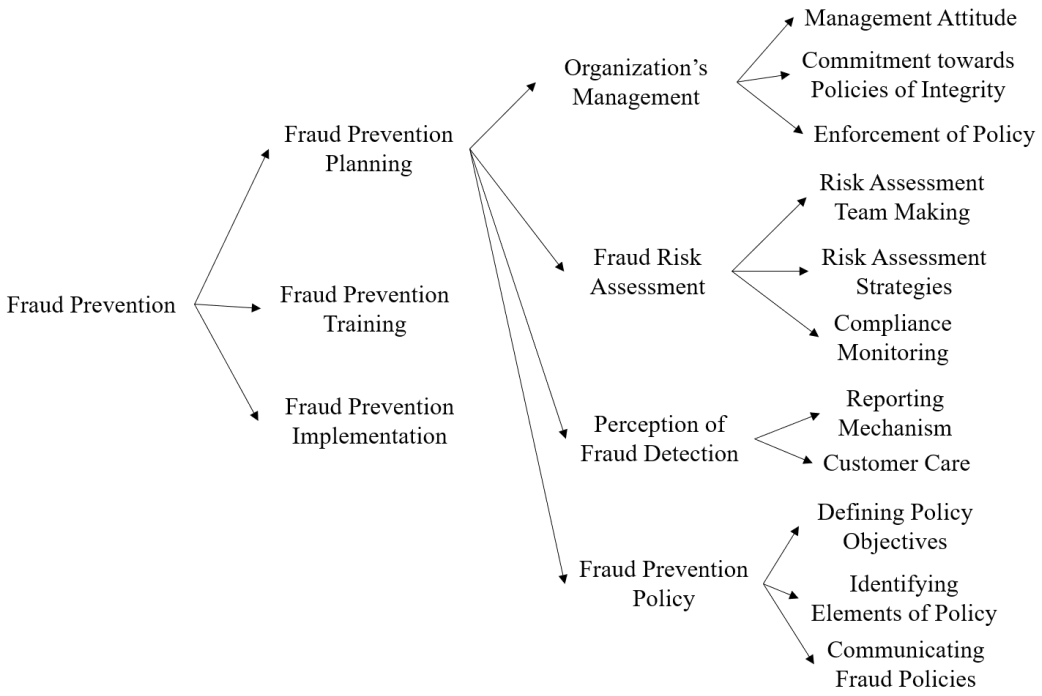

Fig. 1. Basic characteristics.

3) Perception of fraud detection: This phase includes all fraud detection efforts [16–17]. Customer service and fraud reporting are key to this level. Fig. 1 shows that fraud detection and its subsidiary procedures are the fundamental processes in this situation.

4) Fraud prevention policy: The methodical process an organisation follows to create and implement a digital banking fraud prevention policy is called the "fraud prevention policy." This process involves identifying essential fraud policy elements, developing effective communication mechanisms, and rigorously documenting the policy [17]. Fig. 1 shows the three essential subprocesses of creating policy objectives, identifying critical fraud prevention policy elements, and disseminating the fraud policy. It also shows the first step in the fraud prevention policy process.

B. Fraud Prevention Training

Saudi Arabia simulates the fraud prevention approach in this planning phase. At this level, fraud prevention plans and methods are tested and practiced. This involves developing testing processes, creating test scenarios, and carefully assessing the fraud protection plan's performance. Management must also train their Saudi Arabian staff and agents to effectively implement the fraud prevention plan [17].

C. Fraud Prevention Implementation

Saudi Arabian enterprises need comprehensive fraud detection and prevention solutions due to the rising frequency of financial crimes, cyberattacks, and digital fraud. The main goal is to reduce the damage or costs from these illegal operations [17]. Financial crimes, hacking, and digital fraud are on the rise in Saudi Arabia. Organizations can avoid the high costs and consequences of unchecked fraud by implementing efficient fraud detection and prevention methods. This strategic approach protects Saudi Arabian organizations from unbridled fraud [17].

Fraud prevention must be integrated into a comprehensive plan to identify and prevent fraudulent transactions or banking activities in Saudi Arabia, preventing financial and reputational harm to clients and financial institutions. This approach helps identify fraudulent transactions and banking activity and prevent them from harming the Saudi financial sector.

III. Methodology

The proposed methodology for selecting dependable visual analytics tools tailored for medical data analysis in the context of Saudi Arabia is a multifaceted approach encompassing three key phases [5-6]. The methodology commences with the meticulous establishment of a comprehensive network encompassing all variables potentially impacting the problem at hand. This entails a rigorous examination of the entire chain under consideration, with a keen focus on identifying any potential vulnerabilities. Subsequently, the outcomes are categorized based on shared attributes, following the delineation of intersections. This procedural step warrants periodic reevaluation, especially when significant alterations within the chain transpire.

In the subsequent phase, the methodology involves the assignment of weights to the criteria, a crucial step in the process. Intuitionistic fuzzy ANP is the chosen method for this purpose, incorporating the valuable input of domain experts. Within this framework, the criteria are diligently assessed under specific key categories.

The third phase of the methodology encompasses the scrutiny of results derived from multiple criteria evaluations. This comprehensive analysis aids in the identification of key patterns, trends, and insights essential for informed DM.

Finally, the fourth step of the methodology is pivotal in determining the organization’s readiness to employ raw materials. To facilitate this DM process, the intuitionistic fuzzy TOPSIS technique is employed. This step serves as the culmination of the methodology, shaping the organization’s course of action.

In adapting this methodology to the unique landscape of Saudi Arabia, it is paramount to consider the distinct contextual factors, healthcare requirements, and societal aspects that underpin the nation's healthcare sector. The utilization of a reliable knowledge-based fuzzy expert system within this framework holds substantial promise in advancing medical data visualizations, enhancing patient care, and contributing to the evolving healthcare landscape of Saudi Arabia.

A. Intuitionistic Fuzzy ANP

Intuitionistic fuzzy ANP is an extension of ANP that seamlessly incorporates intuitionistic fuzzy set theory into its framework [5-7]. In intuitionistic fuzzy ANP, intuitionistic fuzzy scales are a key part of showing how different parts of different criteria compare in terms of how intense they are. Consequently, this approach enables the creation of an intuitionistic fuzzy decision matrix, with intuitionistic fuzzy quantities representing the ultimate scores assigned to the alternatives [8-10]. By applying specific algebraic operators to these intuitionistic fuzzy integers, the optimal solution is derived, effectively encapsulating the entirety of weight vectors and the judgment matrix.

To gauge the relative importance of one criterion compared to another, intuitionistic fuzzy ANP employs intuitionistic fuzzy numbers in the formulation of an intuitionistic fuzzy judgment matrix for each measure [12-13]. These evaluation vectors, in tandem with the intuitionistic fuzzy pairwise comparison matrix, facilitate the allocation of relative significance to each criterion. The representation of linguistic expressions as intuitionistic fuzzy integers is elucidated in Table I, while Table II delineates the computation of the consistency ratio (CR) through the utilization of the random index (RI). Furthermore, the intuitionistic fuzzy membership function for linguistic terms in both criteria and sub-criteria is visually depicted in Fig. 2.

It is crucial to acknowledge that the final weightings result from a meticulous process of organizing, modifying, and reviewing linguistic term assignments, frequently with the help of expert consensus. By using intuitionistic fuzzy ANP in the context of Saudi Arabia, this method is likely to improve the evaluation of a reliable knowledge-based intuitionistic fuzzy

expert system for medical data visualizations that fits the unique needs of the Saudi healthcare system.

TABLE I. SCALE

Numeric Value	Verbal Value	Intuitionistic based Triangular Fuzzy Number (TFN)
1	Equally significant	1, 1, 3
3	Less significant	1, 3, 5
5	Very significant	3, 5, 7
7	Incredibly Essential	5, 7, 9
9	Extremely Essential	7, 9, 11

TABLE II. SCALE OF RANDOM INDEX

Size (n)	1	2	3	4	5	6	7	8
RI	0	0	0.52	0.89	1.11	1.25	1.35	1.40

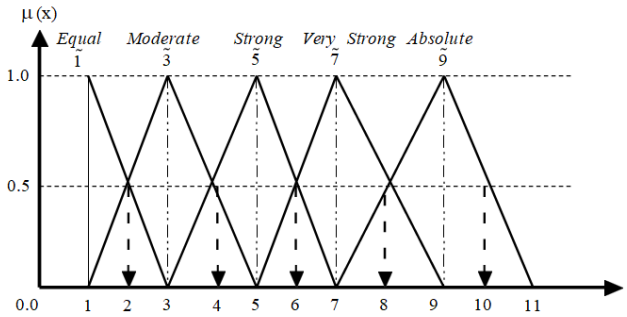

Fig. 2. Function of fuzzy membership.

B. Intuitionistic Fuzzy TOPSIS

Applying intuitionistic fuzzy ANP and intuitionistic fuzzy TOPSIS entails the following three procedures: One must first discover what elements are having an impact on the DM procedure, then perform the calculations for the intuitionistic fuzzy ANP, and finally utilize the intuitionistic fuzzy TOPSIS and Table III to rank the options.

In Saudi Arabia, using intuitionistic fuzzy ANP and intuitionistic fuzzy TOPSIS requires a structured approach that includes three integral procedures. These procedures are delineated as follows: initially, the identification of influential factors affecting the DM process; subsequently, the execution of calculations employing intuitionistic fuzzy ANP; and ultimately, the utilization of intuitionistic fuzzy TOPSIS, along with the insights presented in Table III, to ascertain the ranking of available options.

TABLE III. RATING SCALE

Verbal Values	Equivalent TFNs
Very Poor (VP)	1, 1, 3
Poor (P)	1, 3, 5
Medium (M)	3, 5, 7
Good (G)	5, 7, 9
Very Good (VG)	7, 9, 11

In the initial phase, the identification of potential attributes for the foundational system is conducted. Criteria that hold significance in impacting the DM process are identified, and a hierarchical structure is established to facilitate informed DM. This pivotal phase culminates with the approval of the DM chain of command by the team of decision-makers. An inherent strength of the proposed methodology lies in its adeptness at addressing ambiguity, particularly in terms of criteria and resources. Several key strategies are employed within this method to mitigate or eliminate uncertainty:

Alignment of variables across different facets of the model to gauge the problem-solving capabilities of field experts effectively.

Replacement of numerical data with descriptive terminology through the application of distinct intuitionistic fuzzy membership functions, which are aptly suited for resolving the discussed issues.

Consideration of multiple weighted sources relevant to the subject matter, thereby enhancing the reliability of medical data.

Employing a two-module structure that accommodates varying levels of granularity and uncertainty inherent in medical data sources, encompassing precise qualitative and intangible quantitative medical data, as well as tangible quantitative medical data and data derived from field surveys.

The intuitionistic fuzzy TOPSIS technique demonstrates remarkable efficacy in addressing real-world application challenges within an intuitionistic fuzzy environment. Rooted in traditional multi-attribute-based DM systems, TOPSIS [17] operates on the principle that the alternative selected should be the one farthest from both the positive ideal solution (PIS) and negative ideal solution (NIS). Additionally, TOPSIS features a flexible and user-friendly calculation methodology, enabling the concurrent consideration of multiple criteria with differing units [17]. The procedural steps of the intuitionistic fuzzy ANP-TOPSIS assessment are elaborated below.

Step 1: Determine the relative importance of each criterion for evaluation. In this study, the intuitionistic fuzzy ANP is used to determine preference weights.

Step 2: Build the intuitionistic fuzzy decision/performance matrix and use the criteria to select the right linguistic variables for the different options as shown in Eq. (1) and Eq. (2).

$$\widetilde{DA} = \begin{bmatrix} F_1 \\ F_2 \\ \vdots \\ F_m \end{bmatrix} \begin{bmatrix} f_{11} & f_{12} & \dots & \dots & f_{1n} \\ f_{21} & f_{22} & \dots & \dots & f_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ f_{m1} & f_{m2} & & & f_{mn} \end{bmatrix} \quad (1)$$

i=1,2,3,….m and j=1,2,…n

$$x_{ij} = \frac{1}{K}(x_{ij}^{-1} \oplus \dots \oplus x_{ij}^{-k} \oplus \dots x_{ij}^{-K}) \quad (2)$$

Where x_{ij}^{-k} is performance rating of attribute $A_i$with respect to C_j evaluated by kth expert and $\tilde{x}_{ij}^{k} = (l_{ij}^{k}, m_{ij}^{k}, u_{ij}^{k})$.

Step 3: Next step is constructing the intuitionistic fuzzy decision matrix. The unprocessed medical data are then

normalized by employing a linear scale conversion in order to bring the scales of the different criteria into a comparable format. The intuitionistic fuzzy decision matrix for the attributes $(\widetilde{DA})$ is built as follows Eq. (3) to Eq. (5).

$$(\widetilde{DA}) = [\tilde{d}_{ij}]_{m\times n} \quad (3)$$

Where i=1,2,3,….m and j=1,2,…n

$$\tilde{d}_{ij} = \left(\frac{x_{ij}}{z_j^*}, \frac{y_{ij}}{z_j^*}, \frac{z_{ij}}{z_j^*}\right) \text{ and } z_j^* = \max_i z_{ij} \quad (4)$$

$$\tilde{d}_{ij} = \left(\frac{x_j^-}{z_{ij}}, \frac{x_j^-}{y_{ij}}, \frac{x_j^-}{x_{ij}}\right) \text{ and } z_j^* = \max_i z_{ij} \quad (5)$$

Step 4: Build the weighted and normalized matrix.

Multiplying the weights (wj) of calculating criteria by the normalized intuitionistic fuzzy decision matrix is how one arrives at the weighted normalized matrix (wj) for criteria.$\tilde{d}_{ij}$ see Eq. (6).

$$\tilde{V} = [v_{ij}]_{m\times n} \quad \text{i=1,2,….n ; j=1,2,3……m where } v_{ij} = \tilde{d}_{ij}(\cdot)W_j \quad (6)$$

Note that $\tilde{v}_{ij}$ is a TFN represented by $(\tilde{x}_{ijk}, \tilde{y}_{ijk}, \tilde{z}_{ijk})$

Step 5: Following is the calculation that is used to determine the intuitionistic fuzzy PIS and intuitionistic fuzzy NIS of the attributes as shown in Eq. (7) and Eq. (8):

$$F^* = (\tilde{v}_1^*, \tilde{v}_2^* \dots \dots . \tilde{v}_n^*) \text{ where } \tilde{v}_j^* = (\tilde{z}_j^*, \tilde{z}_j^*, \tilde{z}_j^*) \ \tilde{z}_j^* = \max_i\{\tilde{z}_{ij}\} \quad (7)$$

$$F^- = (\tilde{v}_1^-, \tilde{v}_2^- \dots \dots . \tilde{v}_n^-) \text{ where } \tilde{v}_j^- = (\tilde{x}_j^-, \tilde{x}_j^-, \tilde{x}_j^-) \ \tilde{x}_j^- = \min_i\{\tilde{x}_{ij}\} \quad (8)$$

i=1,2,3…..m; j=1,2,….n

Step 6: The subsequent step is to determine the distance between individual attributes.

The distance (d_i^+, d_i^-) of individual weighted alternative i=1,2,3……m from the intuitionistic fuzzy PIS and intuitionistic fuzzy NIS is computed as per the following in Eq. (9) to Eq. (11):

$$d_i^+ = \sum_{j=1}^n dv(\tilde{v}_{ij}, \tilde{v}_j^+) \quad i = 1, \dots \dots, m \quad (9)$$

$$d_i^- = \sum_{j=1}^n dv(\tilde{v}_{ij}, \tilde{v}_j^-) \quad i = 1, \dots \dots, m \quad (10)$$

$$d(\tilde{A}, \tilde{B}) = \sqrt{\frac{1}{3}((x_A - x_B)^2 + (y_A - y_B)^2 + (z_A - z_B)^2)} \quad (11)$$

Step 7: This step is computation of the closeness coefficient $ClCo_i$ of individual alternative

The closeness coefficient $ClCo_i$ symbolizes the distances to the intuitionistic fuzzy PIS (d^+) and the intuitionistic fuzzy NIS (d^-) concurrently. The closeness coefficient of separate attribute is measured as in Eq. (12):

$$ClCo_i = \frac{d_i^-}{(d_i^+ + d_i^-)} \quad (12)$$

Step 8: Next step is to rank the attributes

In step 8, the values of the maximum closeness coefficient are used to rank or choose the different attributes in decreasing order.

IV. Results

The author evaluates hybrid DM methods for combating digital banking fraud in Saudi Arabia in this part. The author implements intuitionistic fuzzy ANP and shows how it solves selection through hybrid multi-criteria decision-making. The author created and constructed a network of digital fraud prevention model variables and conducted a case study using Saudi-based digital banking applications to evaluate the intuitionistic fuzzy-ANP technique. In addition, the ANP method establishes characteristic weights in phases. 147 Saudi decision-makers and experts evaluated the qualities and options. Three important features, four level 1 characteristics, and eleven level 2 characteristics are compiled from the literature review. After reviewing Saudi Arabian literature and industry standards, the author chose decision network of Fig. 1.

Planning, training, and implementation of fraud prevention are the primary evaluation characteristics. Saudi Arabia's organizational management fraud prevention plan includes fraud risk assessment, perceptions of fraud detection, and fraud prevention policies. Management sub-characteristics include attitude, integrity, and policy implementation. Sub-characteristics of fraud risk assessment include risk assessment teams, methodologies, and compliance monitoring. Customer service and reporting models are fraud detection sub-characteristics. A complete fraud prevention strategy should include planning, training, and implementation. Saudi Arabia uses a matrix to weigh each criterion and alternative.

Consequently, the primary objective of this study is to conduct a case study involving five alternatives (digital fraud prevention models), exploring the attributes that determine their suitability for selecting trustworthy fraud prevention models for the digital banking sector. The chosen approach encompasses a comprehensive set of potential identifiers, each accompanied by rating evaluations. This approach was determined before the commencement of the investigation. The selection of these five digital fraud prevention models as alternatives for comparative trustworthiness evaluation was based on consensus among domain owners and subject matter experts, ensuring a robust evaluation process. To enhance the productivity and reliability of this study, we have conducted an ANP-TOPSIS analysis within an intuitionistic fuzzy framework. This evaluation is centred on assessing the ideality of a hybrid medical expert system for selecting a trustworthy fraud prevention model for the digital banking sector, following the equations detailed in the methodology section, ranging from Eq. (1) to Eq. (12).

After converting linguistic expressions into numerical values Steps 1 to 4 and Eq. (1) to Eq. (6) these values were refined within the intuitionistic fuzzy framework (see Step 5) into clear numerical values. Subsequently, numerical computations were performed to construct a pairwise comparison matrix, with the results summarized in Table IV, as detailed below. The algorithm progressed by introducing intuitionistic fuzzy integer values and then transitioning into crisp numerical values within an intuitionistic fuzzy framework

to present the final results in Table IV. Following that, numerical calculations were executed to generate a pairwise comparison matrix, and the summarized results, which are displayed in Table IV and presented below, are elaborated in the subsequent paragraph.

The method was changed to include intuitionistic fuzzy wrappers as in Eq. (1) to Eq. (5), triangular number estimation, and the degree of possibility in order to get the final results shown in Table V. Ultimately, the experts established the pairwise comparison matrix using Eq. (7) to Eq. (8). Table V showcases the defuzzified values of the group's characteristics, computed using Eq. (9), and the Table V and Fig. 3 were constructed accordingly. Table VI displays the normalized weights of the group's characteristics after calculating local priority vectors, weighted super matrix, and super matrix formation. The comprehensive findings of this investigation are concisely summarized below for reference. After that, numerical calculations were done to figure out the absolute weight vector for row values and figure out which traits were the most important, as shown in Eq. (10) to Eq. (12). The intuitionistic fuzzy data from the judgment matrices were put together to make a pairwise contribution matrix. Table VII and Fig. 4 shows the results of the network as a whole.

TABLE IV. WEIGHTS OF THE CHARACTERISTICS AND THE SUB CHARACTERISTICS

	Characteristics Weight	Sub Characteristics at Level 2	Characteristics Weight	Sub Characteristics at Level 3	Characteristics Weight	Final Weight (CW*SCW3)
Fraud Prevention Planning	0.7200	Organization's Management	0.1601	Management Attitude	0.3312	0.0382
				Commitment towards Policies of Integrity	0.3453	0.0398
				Enforcement of Policy	0.3235	0.0373
		Fraud Risk Assessment	0.3023	Risk Assessment Team Making	0.3111	0.0677
				Risk Assessment Strategies	0.3224	0.0702
				Compliance Monitoring	0.3665	0.0798
		Perception of Fraud Detection	0.2111	Reporting Mechanism	0.3424	0.0520
				Customer Care	0.6576	0.0999
		Fraud Prevention Policy	0.3265	Defining Policy Objectives	0.3222	0.0757
				Identifying Elements of Policy	0.3546	0.0834
				Communicating Fraud Policies	0.3232	0.0760
Fraud Prevention Training	0.1200	-	-	-	-	0.1200
Fraud Prevention Implementation	0.1600	-	-	-	-	0.1600

TABLE V. THE PRIORITY OF THE CHARACTERISTICS

Final Characteristics	Final Weight	Percentage	Overall Priority
Management Attitude	0.0382	3.82 %	12
Commitment towards Policies of Integrity	0.0398	3.98 %	11
Enforcement of Policy	0.0373	3.73 %	13
Risk Assessment Team Making	0.0677	6.77 %	9
Risk Assessment Strategies	0.0702	7.02 %	8
Compliance Monitoring	0.0798	7.98 %	5
Reporting Mechanism	0.0520	5.20 %	10
Customer Care	0.0999	9.99 %	3
Defining Policy Objectives	0.0757	7.57 %	7
Identifying Elements of Policy	0.0834	8.34 %	4
Communicating Fraud Policies	0.0760	7.60 %	6
Fraud Prevention Training	0.1200	12.00 %	2
Fraud Prevention Implementation	0.1600	16.00 %	1

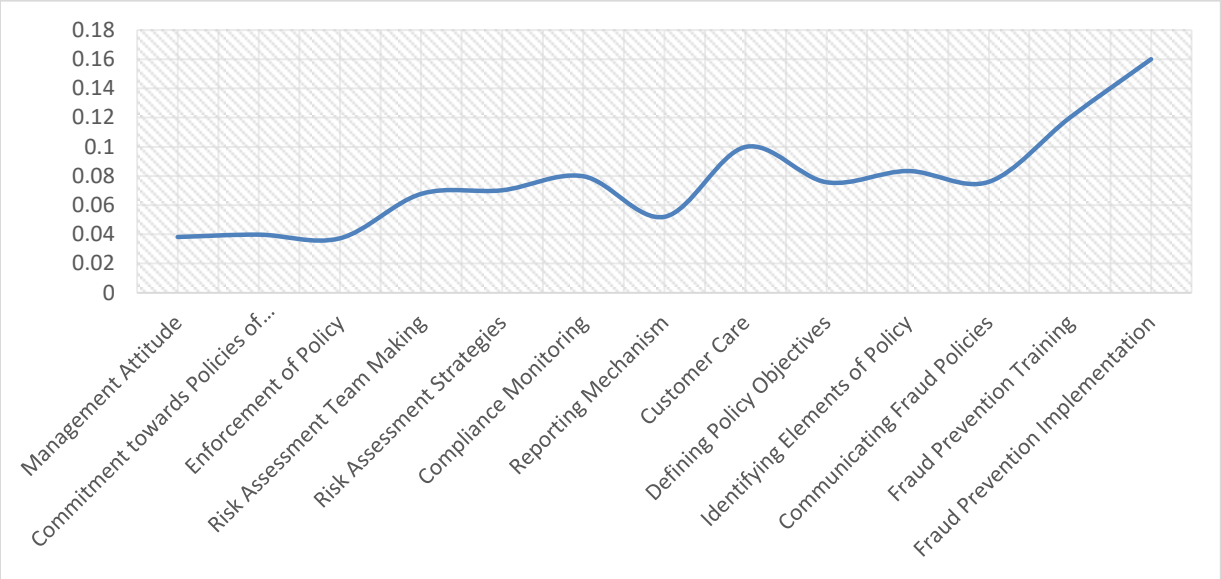

Fig. 3. Graphical representation of characteristics.

Subsequently, the following section of this study will provide a practical assessment of the findings, focusing on the evaluation of a trustworthy fraud prevention model for the digital banking sector. To accomplish this, an ANP approach was applied under conditions of fuzziness to derive the composite weights of features. Subsequently, the intuitionistic fuzzy TOPSIS method was employed to determine the overall ranking of competing alternatives, utilizing the feature weights obtained earlier. It is important to note that these evaluations are particularly relevant in the context of Saudi Arabia.

After completing several intermediary steps, we obtained the normalized intuitionistic fuzzy decision matrix for five fraud prevention models: Riskified [1], Nudata Security [2], GBG Services [18], Feedzai [19], and Featurespace [20]. The results of our analysis are encapsulated within this matrix. To calculate the normalized performance values of the intuitionistic fuzzy decision matrix, we utilized Eq. (8) to Eq. (9). Table VI presents the definitive findings, computed by applying Eq. (10) to Eq. (11) to establish the positive and negative idealness of each alternative concerning each characteristic. These equations were combined to ascertain the ideality of each alternative. The presentation of these results follows the chronological order in which they were obtained.

Furthermore, Eq. (12) were employed to calculate the relative closeness score for each choice, which was then used to determine the degree of satisfaction [21]. The results of this computation can also be found in Table VII and Fig. 4. This additional calculation serves as a valuable post-analysis assessment to provide a comprehensive view of the findings. These evaluations are essential for informed DM in the Saudi Arabian context.

TABLE VI. COMBINED RATINGS WITH RESPECT TO FINAL CHARACTERISTICS

Final Characteristics	Riskified	Nudata Security	GBG Services	Feedzai	Featurespace
Management Attitude	(0.60,0.30,0.40)	(0.65,0.35,0.35)	(0.50,0.30,0.50)	(0.60,0.40,0.40)	(0.55,0.30,0.45)
Commitment towards Policies of Integrity	(0.50,0.30,0.50)	(0.60,0.40,0.40)	(0.70,0.20,0.30)	(0.75,0.20,0.25)	(0.60,0.30,0.40)
Enforcement of Policy	(0.70,0.20,0.30)	(0.75,0.20,0.25)	(0.55,0.30,0.45)	(0.85,0.30,0.20)	(0.75,0.20.0.30)
Risk Assessment Team Making	(0.55,0.30,0.45)	(0.85,0.30,0.20)	(0.60,0.40,0.40)	(0.65,0.30,0.35)	(0.60,0.25,0.40)
Risk Assessment Strategies	(0.60,0.40,0.40)	(0.65,0.30,0.35)	(0.65,0.35,0.35)	(0.60,0.20,0.40)	(0.50,0.40,0.50)
Compliance Monitoring	(0.65,0.35,0.35)	(0.50,0.30,0.50)	(0.60,0.40,0.40)	(0.55,0.30,0.45)	(0.60,0.45,0.40)
Reporting Mechanism	(0.50,0.30,0.50)	(0.60,0.40,0.40)	(0.55,0.30,0.45)	(0.60,0.30,0.40)	(0.60,0.40,0.40)
Customer Care	(0.70,0.20,0.30)	(0.75,0.20,0.25)	(0.60,0.30,0.40)	(0.75,0.20.0.30)	(0.65,0.30,0.40)
Defining Policy Objectives	(0.55,0.30,0.45)	(0.85,0.30,0.20)	(0.50,0.30,0.50)	(0.60,0.40,0.40)	(0.55,0.30,0.45)
Identifying Elements of Policy	(0.50,0.30,0.50)	(0.60,0.40,0.40)	(0.55,0.30,0.45)	(0.75,0.20,0.25)	(0.60,0.30,0.40)
Communicating Fraud Policies	(0.70,0.20,0.30)	(0.75,0.20,0.25)	(0.60,0.30,0.40)	(0.85,0.30,0.20)	(0.75,0.20.0.30)
Fraud Prevention Training	(0.55,0.30,0.45)	(0.85,0.30,0.20)	(0.75,0.20.0.30)	(0.65,0.30,0.35)	(0.60,0.25,0.40)
Fraud Prevention Implementation	(0.60,0.40,0.40)	(0.65,0.30,0.35)	(0.60,0.25,0.40)	(0.60,0.20,0.40)	(0.50,0.40,0.50)

TABLE VII. THE OVERALL SCORE OF DIFFERENT ALTERNATIVES

Alternatives	Ideal Best	Ideal Worst	Ideal Best+ Ideal Worst	Degree of Closeness	Ranking
Riskified	0.0600	0.1200	0.1900	0.67895	1
Nudata Security	0.0700	0.1300	0.2100	0.64587	3
GBG Services	0.0800	0.1600	0.2500	0.66985	2
Feedzai	0.1000	0.1100	0.2200	0.61235	5
Featurespace	0.0800	0.1400	0.2000	0.63528	4

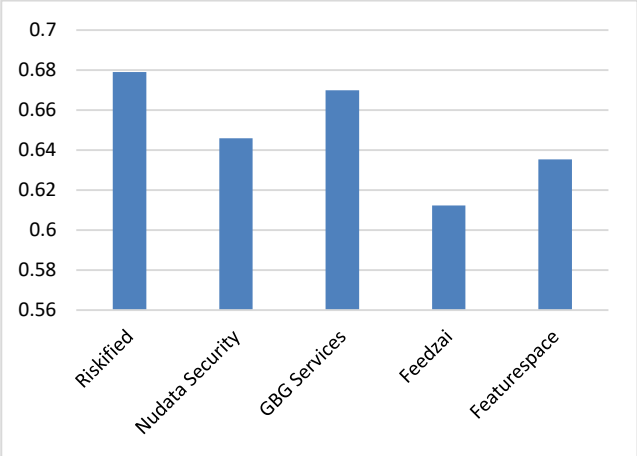

Fig. 4. Impact of alternatives.

The investigation was conducted on five distinct alternatives within the digital banking applications, revealing that categorization is a preferable and successful approach to addressing issues related to fraud prevention in the context of Saudi Arabia. The evaluation was based on the selected characteristics chosen to serve as the foundation for assessment in the Saudi Arabian digital banking landscape.

The relative weights assigned to each of the numerous factors used for selection have a significant impact on the presentation order of various choices. Careful adjustments to the proportional weights of the selection characteristics are essential in the Saudi context to avoid potential ranking changes as a direct consequence of these adjustments. The authors followed a sensitivity analysis approach outlined in [5] to assess the level of confidence in the findings, allowing them to validate their results within the Saudi digital banking environment. By progressively adding a 5% penalty to the weights of each selection criterion one by one, the authors evaluated the sensitivity of the final outcomes to performance variations in Saudi Arabia. These steps enable an exploration of the sensitivity of the results, specifically in the Saudi context. The conclusions derived from the sensitivity analysis are graphically represented in Table VIII and Fig. 5, included for the sake of clarity and convenience for Saudi stakeholders. The results unequivocally demonstrate the ongoing consistency of their practices within the Saudi digital banking sector.

TABLE VIII. SENSITIVITY ANALYSIS

Final Characteristics	Riskified	Nudata Security	GBG Services	Feedzai	Featurespace
Original Outcomes	0.67895	0.64587	0.66985	0.61235	0.63528
Exp-1	0.67789	0.64545	0.66956	0.61985	0.63545
Exp-2	0.67524	0.64756	0.66445	0.61478	0.63458
Exp-3	0.67785	0.64123	0.66658	0.61869	0.64568
Exp-4	0.67265	0.64444	0.66236	0.61856	0.60562
Exp-5	0.67456	0.64445	0.66789	0.61478	0.63789
Exp-6	0.67256	0.64666	0.66985	0.61689	0.63852
Exp-7	0.67235	0.64555	0.66563	0.61658	0.63548
Exp-8	0.67474	0.64223	0.66236	0.60256	0.63658
Exp-9	0.67111	0.64289	0.66745	0.61567	0.63653
Exp-10	0.67874	0.64789	0.66569	0.61856	0.63789
Exp-11	0.67744	0.64987	0.66265	0.61789	0.63356
Exp-12	0.67000	0.64256	0.66485	0.61456	0.63897
Exp-13	0.67446	0.64998	0.67856	0.62568	0.63564

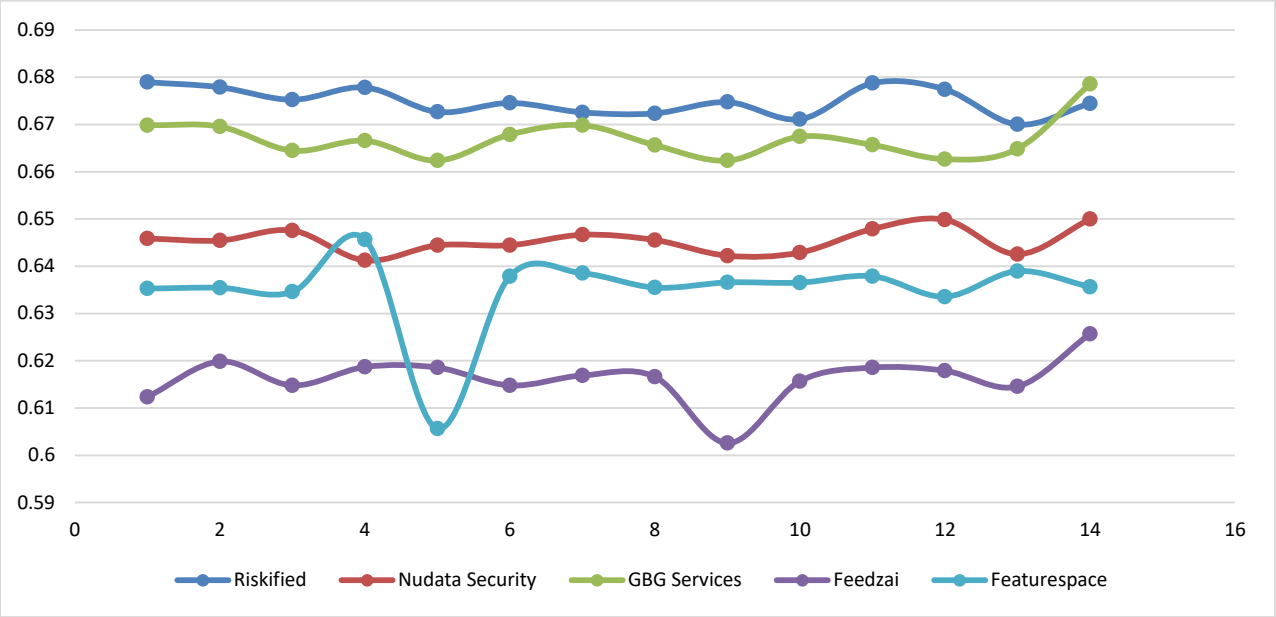

Fig. 5. Graphical representation of sensitivity analysis.

V. Conclusion

This study sheds light on the profound impact of financial theft on Saudi Arabia's economy and culture, underscoring the considerable financial strain it places on individuals. The complex business landscape in the Kingdom of Saudi Arabia (KSA) poses challenges for traditional methods of digital banking fraud detection. Our research set out with several objectives, with a primary emphasis on developing robust DM models within the Saudi financial sector, specifically geared toward effective fraud detection and prevention. Through the application of a novel intuitionistic fuzzy-based DM approach, we aimed to create models capable of assessing fraud detection and prevention in Saudi digital banking systems. The outcomes presented in this paper highlight the efficacy of our proposed approach in detecting and preventing fraud in Saudi Arabian digital banking applications, surpassing the performance of both fuzzy ANP and conventional ANP models. As a final recommendation, we advocate for the implementation of an artificial intelligence (AI) DM program to mitigate fraud in Saudi Arabia. Given the hybrid nature of DM processes in Saudi Arabia, such an algorithm holds promise for significantly enhancing effectiveness and application, ultimately playing a vital role in fortifying fraud protection within the dynamic landscape of KSA's digital banking ecosystem.

Acknowledgment

This research was supported by Arab Open University (AOU)/ KSA. Author is thankful for providing the fund to carry out the work.

References

[1] Unleash your ecommerce growth, Riskified, [Online]. Available at: https://www.riskified.com/.

[2] Trust the person behind the device, Nudatasecurity, [Online]. Available at: https://nudatasecurity.com/.

[3] AffairsCloud YouTube Channel, Affairscloud, [Online]. Available at: https://www.youtube.com/channel/UCkpXde9qr9rmEB1mWGfzfIQ/videos.

[4] D. Krause, "Mitigating Risks for Financial Firms Using Generative AI Tools," SSRN, [Online]. Available at: https://ssrn.com/abstract=4452600.

[5] Penetration rate of online banking in Saudi Arabia from 2013 to 2028, Statista. [Online]. Available at: https://www.statista.com/forecasts/1150349/online-banking-penetration-forecast-in-saudi-arabia.

[6] Payments Fraud and Control Report, J.P. Morgan, [Online]. Available at: https://www.jpmorgan.com/content/dam/jpm/commercial-banking/insights/cybersecurity/highlights-afp-2022-payments-fraud-and-control-report.pdf

[7] A. K. S. Yadav and M. Sora, "Fraud detection in digital banking using text mining models: A review," IOP Conference Series: Materials Science and Engineering, vol. 1020, no. 1, p. 012012, 2021.

[8] S. Chen, "Detection of fraudulent digital banking using the hybrid data mining approach," SpringerPlus, vol. 5, no. 1, pp. 1-16, 2016.

[9] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," Statistical Science, vol. 17, no. 3, pp. 235-255, 2002.

[10] C. Phua, D. Alahakoon, and V. Lee, "Minority report in fraud detection: classification of skewed data," ACM SIGKDD Explorations Newsletter, vol. 6, no. 1, pp. 50-59, 2004.

[11] P. Ravisankar, V. Ravi, G. R. Rao, and I. Bose, "Detection of digital banking fraud and feature selection using data mining techniques," Decision Support Systems, vol. 50, no. 2, pp. 491-500, 2011.

[12] J. N. Dharwa and A. R. Patel, "A data mining with a hybrid approach-based transaction risk score generation model (TRSGM) for fraud detection of online financial transactions," International Journal of Computer Applications, vol. 16, no. 1, pp. 18-25, 2011.

[13] Z. Zojaji, R. E. Atani, and A. H. Monadjemi, "A survey of credit card fraud detection techniques: data and technique-oriented perspective," arXiv preprint arXiv:1611.06439, 2016.

[14] W. Y. Moon and S. D. Kim, "Adaptive fraud detection framework for fintech based on machine learning," Advanced Science Letters, vol. 23, no. 10, pp. 10167-10171, 2017.

[15] R. Wedge et al., "Solving the false positives problem in fraud prediction using automated feature engineering," in Machine Learning and Knowledge Discovery in Databases: European Conference, ECML PKDD 2018, Dublin, Ireland, September 10–14, 2018, Proceedings, Part III, pp. 372-388, Springer International Publishing, 2019.

[16] B. Stojanović et al., "Follow the trail: Machine learning for fraud detection in Fintech applications," Sensors, vol. 21, no. 5, p. 1594, 2021.

[17] T. Pi, H. Hu, J. Lu, and X. Chen, "The analysis of Fintech risks in China: Based on fuzzy models," Mathematics, vol. 10, no. 9, p. 1395, 2022.

[18] Every day we build, collaborate and partner to create a world where everyone can transact online with confidence, Gbgplc, [Online]. Available at: https://www.gbgplc.com/en/about-us/.

[19] Transactin Trust, Feedzai, [Online]. Available at: https://feedzai.com/.

[20] Game-changing innovation. Generative AI for good., Featurespace, [Online]. Available at: https://www.featurespace.com/.

[21] M. Taqi et al., "Village fund financial fraud prevention model using the analytical network process model," Jurnal Organisasi dan Manajemen, vol. 17, no. 2, pp. 203-216, 2021.