International Review of Management and Marketing

ISSN: 2146-4405

available at http: www.econjournals.com

International Review of Management and Marketing, 2026, 16(2), 236-243.

Enhancing Data Privacy and Fraud Detection in the Takaful Industry through Digital Platforms and E-Knowledge Sharing: Moderating Role of AI Adoption

Mansoor Ahmad Qazi[1]*, Maizaitulaidawati Binti MD Husin[2]

[1]PhD Student, Azman Hashim International Business School, UTM, Malaysia, [2]Azman Hashim International Business School, Universiti Teknologi, Malaysia. *Email: mansoorqazi@graduate.utm.my

Received: 30 August 2025 **Accepted:** 23 Decemebr 2025 **DOI:** https://doi.org/10.32479/irmm.22265

ABSTRACT

This research explored the factors essential to data privacy and security in takaful institutions and proposed digital platforms (DPs) to enhance them, mediated by E-knowledge sharing. Moreover, the moderating role of AI adoption on the connection between E-knowledge sharing and data privacy and fraud detection has also been tested. The current study was conducted across various takaful (Islamic insurance) institutions in the United Arab Emirates (UAE) using a survey. Online questionnaire forms were used to collect data, which were subsequently analysed using statistical techniques, including correlation, partial least squares structural equation modelling, and bootstrapping, yielding several interesting results for the formulated hypotheses. The findings confirm the prediction that digital platforms can enhance data privacy and fraud detection. Moreover, the findings confirmed the mediating role of E-sharing in the direct effects of digital platforms, data privacy, and fraud detection. Finally, the findings revealed that AI adoption strengthens the connection between E-knowledge sharing and data privacy, as well as fraud detection.

Keywords: Digital Platforms, E-Knowledge Sharing, Artificial Intelligence Adoption, Data Privacy and Fraud Detection, Takaful Institutions
JEL Classifications: G22; O33; M15

1. INTRODUCTION

Information technology has revolutionised almost every aspect of our lives. It is the lifeblood of the economy in today's world (Ximei et al., 2022; Hamid et al., 2024). Nowadays, with the widespread use of technology across every field of life, takaful institutions (Islamic insurance) are not left behind (Hassan et al., 2023). No doubt, Information Technology has been used in Takaful institutions for many years. Still, it has gained significant importance for data protection and fraud detection, where technology has reached new heights (Gazali et al., 2023). In today's world, it is impossible to imagine a world without technology; it's crucial in every aspect of life (Ahmad et al., 2023). The use of technology in Takaful institutions enhances the efficiency and effectiveness of customer service (Mehboob et al., 2025). Technology is rapidly changing the world today, including the Takaful industry, as it provides new opportunities by strengthening traditional service methods into digital services (Kondapaka, 2021).

The takaful institutions have been experiencing faster digital transformation as service providers deploy DPs for underwriting, claim handling, sales, and partner integrations to expand reach and improve service efficiency (Wahyuni, 2022). DPs create comprehensive, high-volume, diverse customer and transaction data that can drive unconventional analytics and quick decision-making (Bonina et al., 2021). At the same time, DPs raise exposure to third-party sharing, cross-border information flows, and profiling (privacy risks), as well as to different practices of digitally enabled fraud that exploit platform communications and automated procedures (Ahmad et al., 2023). These pressures, such as data privacy and improving fraud detection, become central operational concerns for takaful firms.

Data privacy and fraud detection have become essential for takaful institutions in the era of digitalisation (Memon et al., 2024). The Takaful industry has experienced rapid digitalisation as takaful management pursues better customer services, lower average costs, and broader access to the target market through DPs (Tambi and Rahman, 2023). DPs generate opportunities such as claims automation, real-time underwriting, and better distribution channels for Takaful institutions (Ramachandaran et al., 2025); on the other hand, they also significantly increase the velocity, volume, and variety of customer and transactional data administered by Takaful operators. The use of advanced technologies for transactional data raises two-fold concerns: Data privacy (protecting sensitive financial and personal data) and the prevention of sophisticated, digitally enabled fraud (Kasim et al., 2025).

It is self-evident that DPs and E-knowledge sharing mechanisms (e.g., agent portals, internal knowledge management systems, and cross-partner knowledge exchanges) can enhance fraud screening and operational learning (Dong et al., 2024).Takaful institutions also pose new confidentiality risks (e.g., data sharing with third parties, behavioural reporting) and leave gaps in traditional fraud controls. The Takaful sector faces a serious challenge: Connecting DPs and e-knowledge sharing to support fraud detection (Kasim et al., 2015), without compromising compliance with data protection standards and participant trust, particularly in jurisdictions with specifictakaful data codes (Awosika et al., 2023). In this regard, AI adoption provides powerful tools for automated decision-making, pattern detection, and anomaly scoring, thereby significantly enhancing the precision and timeliness of fraud detection (Benedek et al., 2022). Simultaneously, AI systems offer control over bias and privacy-protective techniques (e.g., differential privacy and federated learning). This suggests that AI adoption may strengthen the relationship between data privacy and fraud control (Malhotra et al., 2004). With AI, platform-enabled data can be more effectively transformed into fraud indicators (Singh and Gupta, 2014), but AI must be implemented and managed correctly to avoid privacy issues.

Likewise, we argue that the connection between DPs and data privacy is a composite rather than straightforward. Because it involved the preparation and collection of data using DPs, organisational E-knowledge sharing is a crucial factor for data privacy (Hassan et al., 2018). E-knowledge sharing activities enable the receipt of data and information from participants via online platforms, allowing for the adjustment of information to ensure privacy (Aslam et al., 2023). The e-knowledge sharing mechanism consists of agent portals, case libraries, structured inter-firm intelligence exchanges, and internal claim knowledge bases (Benedek et al., 2022). Existing studies in the field of knowledge management have empirically found that E-knowledge sharing advances frontline decision-making, supports the codification of fraud typologies, and reduces detection latency, particularly when coupled with analytics (Ali, 2021). The exchange of information between operators and participants appears to yield several benefits, such as operationalising fraud intelligence and privacy controls (Hassan et al., 2023). Therefore, the current study also investigates the mediating role of E-knowledge sharing between DPs and the data privacy link.

2. LITERATURE REVIEW

2.1. Digital Platforms, Data Privacy, and Fraud Detection

DPs in Takaful (insurance) act as marketplaces, orchestrators, and data centres that enable the transformation of how operators cooperate and communicate with customers, third-party data providers, and distribution partners (Nugroho and Apriantoro, 2025). Platform environments allow rapid data accumulation, facilitating innovative analytics, but they also increase attack surfaces and third-party exposure (Cenamor et al., 2017). Existing studies in the context of takaful have mostly emphasised both the potential benefits and associated risks, including privacy breaches and multifaceted liability chains across participants on established platforms (Bonina et al., 2021). DPs mechanism provides ridiculous feedback for fraud detection but increases data privacy and control complications (Hamid et al., 2024; Smith et al., 1996).

Though DPs such as e-knowledge networks, agent portals, and internal knowledge bases (Ahmad et al., 2023) have the potential to enhance fraud detection by enabling the rapid spread of fraud typologies and associated signals, and by facilitating unauthorised data exposure (Memon et al., 2024), the takaful operators increase fraud detection and maintain adequate data privacy using DPs (Kondapaka, 2021). DPs in takaful act as a multi-network that aggregates agents, customers, third-party services and data providers (Gazali et al., 2023). For takaful, DPs' adoption supports participants and agents in the distribution of data, processing of claims, and real-time telemetry (Hassan et al., 2023), but also increases the risk of data privacy breaches.

Fraud detection is an additional persistent issue in digitalized takaful activities (Wahyuni, 2022). The global insurance industry faces numerous frauds annually (Tambi and Rahman, 2023), and takaful institutions also encounter similar problems, including fraudulent claims, agent misreporting, and identity manipulation (Kasim et al., 2015). In this regard, DPs can enable earlier fraud detection by accumulating information and distributing fraud typologies across various units of entities (Vuković et al., 2025). The following hypotheses were developed.

H_1: DPs are significantly linked with data privacy and fraud detection in takaful institutions.

2.2. Digital Platforms and E-Knowledge Sharing

DPs can offer a practical framework and provide networks connecting companies to the platform, enabling business organisations to assimilate, gather, and govern material and data on the platform (Helfat and Raubitschek, 2018). It is the unique features of self-growth classification, network consequences, and modularisation that constitute well-organised means for enterprises to obtain rapid information about participants (Faqih and Nurhayati, 2023). DPs could enable organisations to obtain resources, strategic flexibility, and dynamic, essential collaboration, allowing them to leverage DPs' procedural characteristics to acquire and integrate key information (Nugroho and Apriantoro, 2025). Hence, with improvements in the DPs, enterprises can more efficiently facilitate knowledge sharing among parties, leading to

better decision-making (Cenamor et al., 2017; Mohy-Ul-Din et al., 2019). Organizations sustain their dynamic capability by extracting substantial information and estimating participants' preferences and trends (Venkatesh et al., 2003). DPs enable organisations to assemble critical shared knowledge to respond promptly and dynamically to market requirements (Elgargouh et al., 2024). DPs refer to the capacity of an organization to sustain relationships with users through online marketing, communication, and collaboration, enabling low-cost and advanced resource expansion (Hassan et al., 2023; AlNemer, 2025).

H_2: DPs are significantly linked with e-knowledge sharing in takaful institutions.

2.3. Mediating Role of E-Knowledge Sharing

DPs and their application become means of knowledge and evidence in takaful organisations (Hellemans et al., 2021). Likewise, e-knowledge sharing enables enterprises to collect and share a variety of information that supports practical activities primarily related to data privacy and fraud detection (Hussain et al., 2025). If an organisation can improve its digital networks to shape its services, it is more likely to develop modern digital solutions that advance customer value and trust (Bonina et al., 2021). DPs offer organisational flexibility and dynamic digital capabilities that can enhance their operations and services, thereby improving performance (Kazan et al., 2018). A company that possesses DPs will have greater e-knowledge sharing, thereby achieving enhanced data protection in customer services (Kurdi, 2024). DPs are a set of networks that utilise digital properties to generate divergence values; these digital properties include IT competencies to enhance performance (Ali, 2021). However, the extent of the linkage between DPs and data protection and privacy hasn't been extensively examined, particularly from the perspective of e-knowledge sharing. DPs provide a foundation for knowledge-sharing activities in an organisation (Nugroho and Apriantoro, 2025). Hence, the present investigation suggests that e-knowledge sharing serves as a mediating factor between DPs and data privacy and fraud detection.

Most takaful institutions gain a significant advantage from their DPs, thanks to advanced tools and e-knowledge sharing, as well as significantly developed communication methods (Dong et al., 2024). E-knowledge sharing enhances data privacy and fraud detection by introducing novelty into both enterprise practices and services (Parhi et al., 2025). E-knowledge sharing plays a critical role in fraud detection. The existing KM literature suggests that controlled e-knowledge sharing accelerates fraud identification by leveraging best practices and fraud typologies (Elgargouh et al., 2024). DPs enhance e-knowledge sharing to enhance data privacy and improve fraud detection (Cosma and Rimo, 2024). Recent KM studies in takaful institutions highlighted that organised knowledge flows facilitate better decision-making and can decrease recognition latency when combined with analytics (Stewart and Segars, 2002). The DPs assist takaful companies in building relationships with various participants, which ultimately enhances performance and data privacy (Awosika et al., 2023). Thus, this study argues that DPs play a foundational role in e-knowledge sharing, thereby improving data privacy and fraud detection.

H_3: E-knowledge sharing is significantly linked with data privacy and fraud detection in takaful institutions.

H_4: E-knowledge sharing significantly mediates the association between DPs and data privacy and fraud detection in takaful institutions.

2.4. Moderating Role of AI Adoption

The adoption of AI becomes a serious issue for takaful institutions in the era of digitalisation (Benedek et al., 2022). Developing the E-services of takaful institutions is a pressing need to initiate digital activities to address the risks associated with technology (Aslam et al., 2023). Takaful institutions successfully respond to these changes by developing DPs and sharing E-knowledge to leverage existing human, technological, and financial resources (Adam et al., 2018). In the digital era, DPs and E-knowledge sharing support in addressing emerging risks, such as data privacy and fraud detection through AI adoption (Kondapaka et al., 2021). DPs and E-knowledge sharing within takaful institutions gain importance as they adopt AI. AI adoption primarily concerns the takaful institutions' ability to address emerging challenges and risks arising from digitalisation through e-knowledge sharing and DPs (Ahmad et al., 2023). Although researchers such as Mehboob et al. (2025) explored the effects of DPs on AI adoption, few examined the roles of e-knowledge sharing and AI adoption in data privacy and fraud detection more generally.

E-knowledge sharing enables takaful institutions to drive AI adoption amid technological and digitalisation challenges and risks, including data privacy and fraud detection (Hassan et al., 2018). E-knowledge sharing facilitates the acquisition of key knowledge necessary to enhance takaful services. E-knowledge sharing comprises various technological devices that aim to edit, standardise, and allocate internal and external data in exceptional ways (Williamson, 2021). With sound AI adoption, organisations can secure a competitive position in the relevant industry and data privacy and fraud detection (Gazali et al., 2023). AI adoption process promoted through knowledge of various stakeholders, including participants, agents, and third-party data providers (Ximei et al., 2022).

Empirical studies suggest that AI adoption in takaful institutions is driven by readiness, technical capabilities, and governance (Singh and Gupta, 2014). In takaful institutions, AI adoption plays a moderating role on the connection between e-knowledge sharing and fraud/privacy outcomes. Established AI adoption with a privacy-by-design approach may support optimistic consequences, whereas undeveloped adoption may exacerbate risks. The current study formulated that:

H_5: AI adoption significantly moderates the association between e-knowledge sharing and data privacy and fraud detection in takaful institutions.

2.5. Theoretical Framework

The current study formulated hypotheses to predict DPs for e-knowledge sharing, data privacy, and fraud detection. The current study also examined the mediating role of e-knowledge sharing in the relationship between data privacy and fraud detection. Finally,

we also hypothesised that AI adoption moderates the association between e-knowledge sharing and data privacy and fraud detection. Figure 1 shows the theoretical framework.

3. METHODOLOGY

The nature of the current study was descriptive, which confirms the use of a cross-sectional design. A cross-sectional design allows researchers to collect data from respondents at a single point in time. We used an online survey to collect responses from study participants. The target population consists of managers, IT specialists, risk officers, and compliance officers directly involved in DPs and fraud detection initiatives working in takaful institutions served in the UAE (including Abu Dhabi, Dubai, Fujairah, Umm Al Quwain, Sharjah, Ras Al Khaimah and Ajman), For data collection the services of 4 research assistants was employed for higher response rate. Questionnaires were mailed to 348 agents of 10 takaful institutions, but only 283 responses were received. After excluding incomplete responses, only 267 questionnaires were used for analysis. Table 1 shows the respondent characteristics.

3.1. Study Measures

The measurement items for the constructs of the current study were based on previous studies on DPs, e-knowledge sharing, AI adoption, and data privacy and fraud detection. All the measures were adopted from the prior work of other researchers. DPs are used as a predictor of data privacy and fraud detection. An eight-item scale, modified from the work of Rai and Tang (2010) and Cosma and Rimo (2024), was used to measure DPs as an independent variable. The assessment includes online mechanisms, knowledge exchange platforms, blogs and forums for the acquisition and dissemination of knowledge, which are key components of DPs measurement.

E-knowledge sharing is used as a mediating variable between DPs and data privacy and fraud detection. The 4-item scale used to measure e-knowledge sharing was taken from Gold et al. (2001), Zhang et al. (2024) and Elgargouh et al. (2024). Evaluating the exchange of knowledge, training, and educational expertise with others led to the development of novel ideas.

The outcome variable, i.e., data privacy and fraud detection, is measured using 06 items adopted from Smith et al. (1996), Malhotra et al. (2004), and Bhattacharya et al. (2025). Finally, AI adoption is measured as a moderating variable using a 6-item scale from the work of Singh and Gupta (2014) and Venkatesh et al. (2003).

4. RESULTS

Collected data were analysed with SPSS (Statistical Package for the Social Sciences) version 23 and SEM. A two-step SEM approach is applied in AMOS 24.0, with the first step used to examine the measurement model using validity, factor loadings, and reliability of the study constructs. The second step examined the hypothesised relationship with the structural model. In the first step of data analysis, confirmatory.

Factor analysis (CFA) was performed to examine the uniqueness of the constructs, i.e., DPs, e-knowledge sharing, AI adoption, and data privacy and fraud detection. CFA was conducted with four models with different specifications. The outcomes of CFA are presented in Table 2. The outcomes of the model with four factors met the acceptance criteria, $\chi^2 = 1032.52$, CFI = 0.92, GFI = 0.94, RMSEA = 0.05.

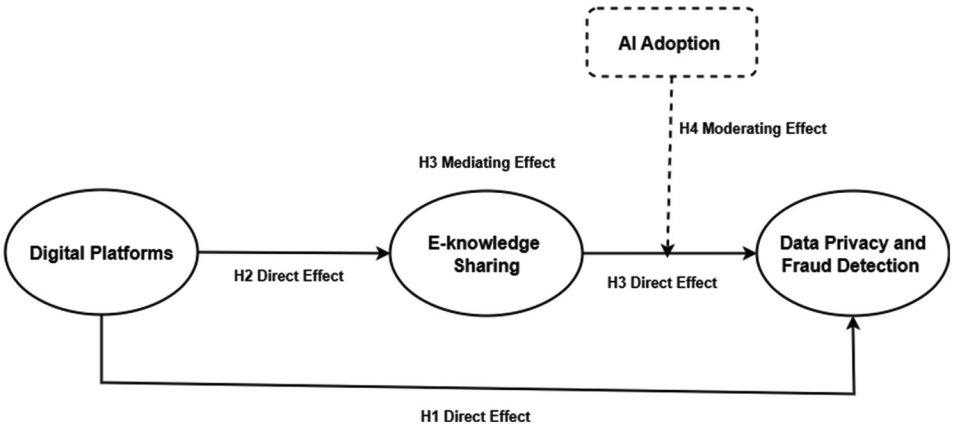
4.1. Reliability and Validity Analysis

To establish the validity and reliability of the adopted constructs, we conducted reliability and validity tests to obtain AVE, factor loadings, and Cronbach's alpha. Table 3 presents the results of the validity and reliability tests. According to the value, the validity

Table 1: Demographics

Controlled variables	n	%
Gender		
Male	199	74.53
Female	68	25.47
Age (in years)		
18-22	170	63.67
Above 22	97	36.33
Qualification in years		
14	134	50.19
16	104	38.95
More than 16	29	10.86

Figure 1: Conceptual model and hypotheses of the research



and reliability of the study measures were established, as they met the acceptance criteria and thresholds for validity and internal consistency.

Table 4 contained the results of the correlation among study variables. The findings revealed that DPs have significant direction towards E-knowledge sharing (0.39*) and data privacy and fraud detection (0.38*). Moreover, the findings also showed that E-knowledge sharing has a significant direction towards AI adoption (0.33*) and data privacy and fraud detection (0.35*). Furthermore, AI adoption also has a considerable impact on data privacy and fraud detection (0.31*), respectively.

4.2. Hypotheses Testing

To verify the hypothesis H_1, path analysis was used; for hypothesis H_2 (the mediating role of E-knowledge sharing), we followed Preacher and Hayes'' approach (2008), and for the hypothesis H_3 (the moderating effect of AI adoption), A hierarchical regression analysis da Silva Faia and Vieira, 2018) was employed. The second step of SEM examined the hypothesised relationships using a structural model. The current study (H_1) was formulated to predict DPs for data privacy and fraud detection. The coefficients presented in Table 5 from the path analysis confirm the optimistic prediction of DPs for data privacy and fraud detection. These findings revealed that DPs play a foundational role in enhancing data privacy and fraud detection. The direct path from DPs to data privacy and fraud detection generates a coefficient of 0.26. Based on these findings, we accept the study's H_1.

The current study's (H_2) was formulated to predict DPs for E-knowledge sharing. The coefficients in Table 5 from the path analysis confirm the optimistic predictions of DPs regarding E-knowledge sharing. These findings revealed that DPs play a foundational role in enhancing E-knowledge sharing. The direct path from DPS to E-knowledge sharing generates a coefficient (0.30). Based on these findings, we accept the study's H_2.

The current study (H_3) was formulated to predict E-knowledge sharing for data privacy and fraud detection. The coefficients in Table 5 from the path analysis confirm the positive association between E-knowledge sharing and data privacy and fraud detection. These findings revealed that E-knowledge sharing plays a critical role in enhancing data privacy and fraud detection. The direct path from E-knowledge sharing to data privacy and fraud detection generates a coefficient (0.28). Based on these findings, we accept the study's H_3.

E-knowledge sharing mediates the relationship between DPs and data privacy and fraud detection DPs→E-knowledge sharing data privacy and fraud detection). Using the Preacher and Hayes analysis process, the results confirm the indirect effect of E-knowledge sharing between DPs on data privacy and fraud detection (Beta = 0.22, L = 0.2891, U = 0.2922). The findings are presented in Table 6. We accept the study's H_4.

4.3. Moderation Analysis

Hierarchical regression analysis was employed in three steps for the moderation analysis. Table 7 presents the results of the regression analysis testing the moderating effect of AI adoption. In the first step, we regressed the independent variable, yielding a significant coefficient (0.39). In the second regression, we regress the independent variable (E-knowledge sharing) and

Table 2: Confirmatory factor analysis (CFA)

Model detail	χ2	Df	χ2/df	RMESA	GFI	CFI
Hypothesized four-factor model	1032.52	475	2.174	0.05	0.94	0.92
Three-factor model	1142.56	370	3.088	0.13	0.86	0.83
Two-factor model	1295.35	380	3.409	0.18	0.75	0.72
Single-factor model	1345.34	375	3.588	0.22	0.63	0.61

Table 3: Reliability and validity of the construct

Constructs	Items	Cronbach's alpha	Factor loading	Composite reliability	AVE
DPs	08	0.79	0.73-0.91	0.82	0.68
E-knowledge sharing	04	0.76	0.70-0.88	0.80	0.71
AI adoption	06	0.79	0.73-0.91	0.82	0.68
Data privacy and fraud detection	06	0.81	0.76-0.90	0.84	0.73

Table 4: Correlation

Constructs	Mean	SD	1	2	3	4
DPs	3.9	0.81	1			
E-knowledge sharing	3.3	0.87	0.39*	1		
AI adoption	2.9	0.84	0.28*	0.33*	1	
Data privacy and fraud detection	3.6	0.90	0.38*	0.35*	0.31*	1

Table 5: Path analysis

Paths	Estimates	Standard error	C.R (t-value)
Data privacy and fraud detection ←DPs	0.26	0.063	4.127**
E-knowledge sharing←DPs	0.30	0.057	5.263**
Data privacy and fraud detection ←, E-knowledge sharing	0.28	0055	5.090**

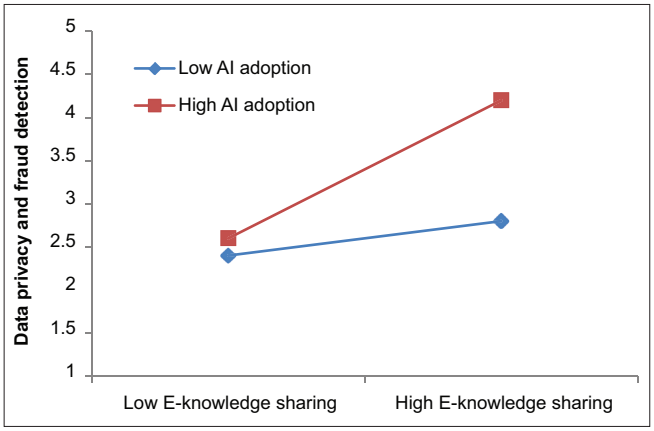
Table 6: Indirect effect of E-knowledge sharing

Model description	Data	Boot	SE	L.V	U.V	Sig
DPs→E-knowledge sharing→ data privacy and fraud detection	0.22	0.23	0.09	0.2891	0.2922	0.000

Table 7: Regression results of the moderating effects of AI adoption

Constructs	Model 1	Model 2	Model 3
E-knowledge sharing	0.39**	0.31**	0.37**
AI adoption		0.30**	0.41**
E-knowledge sharing X AI adoption			0.21*
R^2	0.32	0.36	0.38
Adjusted R^2	0.31	0.33	0.35
Δ R^2	0.32	0.05	0.02
Δ F	291.76**	47.56**	20.98**
N	391	391	391

Figure 2: Slope analysis



the moderating variable (AI adoption) and generated significant values (0.31) and (0.30), respectively. Finally, we added an interaction term (E-knowledge sharing and AI adoption) along with independent variable (DPs) and moderating variable (AI adoption), also generating positive and significant coefficients (0.37), (0.41) and (0.21) respectively. In line with these results, the moderating effect of AI adoption on E-knowledge sharing, data privacy and fraud detection was confirmed; hence, the study's H_5 is accepted.

Moreover, a slope analysis was conducted to examine how the relationship between the independent variable (E-knowledge sharing) and the dependent variable (data privacy and fraud detection) varies across levels of the moderating variable (AI adoption). The slope analysis confirmed that when moderation is significant, the direct effect of the independent variable (E-knowledge sharing) on the dependent variable (data privacy and fraud detection) is not constant, as presented in Figure 2. Slope analysis conducted for the interaction term, i.e. E-knowledge sharing X AI adoption. It is concluded that when AI adoption, along with E-knowledge sharing, is higher, data privacy and fraud detection also increase, and vice versa.

5. DISCUSSION

This study aimed to explore the roles of DPs and E-knowledge sharing in promoting data privacy and fraud detection. Moreover, the moderating effect of AI adoption has been tested for the relationships between E-knowledge sharing, data privacy, and fraud detection. The current study proposes an association among DPs, E-knowledge sharing, AI adoption, and data privacy and fraud detection. H_1 is formulated to predict data privacy and fraud. The findings confirmed that DPs positively predict data privacy and fraud detection, supporting and extending the work of previous studies. These studies elucidated that DPs play a critical role in improving takaful institutions' stance on data privacy and fraud detection. Takaful institutions with the DPs mechanism provide the basic infrastructure necessary to enhance takaful activities, data privacy, and fraud detection. DPs enable agents to acquire the knowledge and skills needed to support data privacy and fraud detection.

H_2 formulated that DPs predict E-knowledge sharing. H_2's findings confirmed the positive effect of DPs on E-knowledge sharing. The DPs regarding takaful services enhance motivation to share information with these institutions. Participants' desire to achieve the desired outcomes increases their willingness and motivation to act towards knowledge sharing. H_3 formulated that E-knowledge sharing predicts data privacy and fraud detection. The findings of H_3 confirmed the positive effect of E-knowledge sharing on data privacy and fraud detection. E-knowledge sharing among various actors within takaful institutions enhances data privacy and fraud detection mechanisms.

The H_4 was formulated to examine the mediation of E-knowledge sharing in the connection between DPs and data privacy and fraud detection. The outcomes of H_4 confirmed that E-knowledge sharing between DPs mediates data privacy and fraud detection. The data privacy and fraud detection are primarily based on the E-knowledge sharing mechanism. Through E-knowledge sharing, takaful institutions acquire information and data support to ensure participants' privacy and data security against fraud. The H_4 proposed for testing the mediation of E-knowledge sharing for the connection between DPs and data privacy and fraud detection. The outcomes of H_4 confirmed that E-knowledge sharing between DPs mediates the effects of data privacy and fraud detection. Moreover, H_5 was formulated for the strengthening role of AI adoption. The results showed that AI adoption plays a critical role in data privacy and fraud detection, thereby increasing participants' confidence. AI adoption enables the takaful faculty to be aware of the collected data on participants for privacy and fraud detection purposes.

5.1. Managerial Implications

The current study also highlighted practical implications for the takaful sector, based on its findings. Promoting takaful institutions and Islamic insurance brings prosperity and growth for emerging economies. The findings imply that takaful institutions should promote takaful activities through DPs that improve takaful standards, leveraging data privacy and fraud detection.

Preparing for takaful activities by Islamic insurance sectors contributes to enhancing the country's economic performance. To achieve data privacy and fraud detection, takaful institutions should consider DPs and an E-knowledge-sharing mechanism to reduce communication gaps. The DPs and e-knowledge-sharing practices that takaful institutions must implement, from the perspective of data privacy and fraud detection, improve participants' risk-taking behaviour. The Takaful sector involved in the DPs becomes more competitive and can utilise resources to improve economic performance by promoting takaful activities. Therefore, management of the takaful sector must focus on DPs and E-knowledge sharing to encourage the takaful stance of various participants.

The perception of data privacy and fraud detection affects the participant's decision. Decision-making authorities, such as the management of the takaful sector, should make necessary adjustments to DPs and AI adoption to improve data privacy and fraud detection. Based on AI strategies for fraud detection, the management of the takaful sector can make informed decisions in response to economic, cultural, and institutional changes,

leading to increased insurance activities among takaful institutions. Management of takaful institutions should formulate IT and AI adoption strategies that ensure takaful activities are conducted at a high level to generate takaful.

5.2. Theoretical Implications

The theoretical implications of this study highlight the crucial role that DPs play in advancing new takaful initiatives. Because there is a direct and advantageous link between DPs and data privacy and fraud detection, it is crucial to promote DPs and awareness-raising campaigns to develop a well-informed public that can make takaful decisions. The results also highlight the vital role of E-knowledge sharing as a mediating mechanism that converts information gained through DPs into practical actions. Participants and agents can utilise the E-knowledge sharing mechanism to exchange information, facilitating the implementation of takaful activities and making a substantial contribution to the promotion of takaful institutions. The current study contributes to the theoretical development of information asymmetry theory (IAT) and the technology acceptance model (TAM) by evaluating how DPs and e-knowledge sharing serve as digital factors that affect data privacy and fraud detection in takaful institutions. The study at hand also extends the diffusion of innovation (DOI) by examining how AI adoption enhances the productive capabilities of takaful institutions.

The key focus of this study is on the DPs, E-knowledge sharing, AI adoption and data privacy and fraud detection in the context of rapid economic transformation and emerging policy support for takaful activities. This study has extended previous research by examining DPs and e-knowledge sharing from the perspectives of DPs and e-knowledge sharing, and their relationships with data privacy and fraud detection in the Western context.

To establish and test a model that connects AI adoption to implications for data privacy and fraud detection, and to enrich knowledge of unexplored outcomes of DPs and E-knowledge sharing from the perspective of a non-Western setting. The mediation role of E-knowledge sharing in our research has advanced the understanding of participants' confidence in translating information into practice. Finally, the findings of this study contradict the existing literature on data privacy and fraud detection in Western and Middle Eastern contexts, as very little prior work has been conducted. The literature suggests that DPs, E-knowledge sharing, and AI adoption can promote insurance activities globally. The findings identified new ways to enhance takaful in the UAE's emerging economy.

5.3. Limitations and Future Research Directions

The study at hand is not without limitations, even though it offers insightful insights into the relationships among DPs, E-knowledge sharing, AI adoption, and data privacy and fraud detection. First, the current study's methodology is cross-sectional, which limits the ability to demonstrate causal relationships, underscoring the need for a longitudinal study to examine temporal interactions. Second, the sample may not accurately reflect the variety of Takaful circumstances, potentially affecting the generalizability of the current study's results. Future studies could investigate how socioeconomic, cultural, and regulatory factors impact the relationships among the variables and utilise more diverse samples.

6. CONCLUSION

The purpose of the study was to explore how digital platforms (DPs) and E-knowledge sharing can help to improve data privacy and fraud detection in the takaful industry, while also examining the moderating role of AI adoption to strengthening these relationships. The findings show that digital platforms are essential and can enhance data privacy and fraud detection. Moreover, the findings confirmed the mediating role of E-knowledge sharing in the direct effects of digital platforms on data privacy and fraud detection, and that takaful institutions that actively use AI technologies gain greater benefits from digital platforms and E-knowledge sharing. In conclusion, improving data privacy and fraud detection in the takaful industry requires not only digital tools but also the integration of digital platforms, E-knowledge sharing, and AI. The study offers practical insights for takaful institutions and policymakers to strengthen digital governance and ensure long-term sustainability in an increasingly digital economy.

7. ACKNOWLEDGEMENT

The author declares that there are no conflicts of interest related to this research. Additionally, the author has no financial interests or competing affiliations that could have influenced the study's design, execution, or findings. This manuscript is the author's original work and has not been previously published or submitted for review to any other journal or conference.

REFERENCES

Adam, K., Bakar, N.A.A., Fakhreldin, M.A.I., Majid, M.A. (2018), Big data and learning analytics in e-learning. Advanced Science Letters, 24(10), 7838-7843.

Ahmad, Z., Mokal, M.N., Rahman, M. (2023), Takaful industry in the era of technological advancement. JEKSYAH Islamic Economics Journal, 3(2), 56-69.

Ali, K.M.M. (2021), TakafulTech for business excellence and customer satisfaction. In: Islamic FinTech: Insights and Solutions. Cham: Springer, p385-403.

AlNemer, H.A. (2025), Participants' knowledge of takaful products in Saudi Arabia. International Journal of Business Economics and Law, 7(1), 43-53.

Aslam, E., Muhammad, R.S., Aslam, M., Iqbal, A., Shabbir, M.S. (2023), Consumer awareness and knowledge of takaful: Evidence from Pakistan. Journal of Namibian Studies, 33, 1-15.

Awosika, T., Shukla, R.M., Pranggono, B. (2023), Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection. [arXiv Preprint].

Benedek, B., Ciumas, C., Nagy, B.Z. (2022), Automobile insurance fraud detection in the age of big data: A systematic review. Journal of Financial Regulation and Compliance, 30(4), 503-523.

Bhattacharya, A., Basumatary, H., Deb Barma, M.K. (2025), Privacy in next-generation wireless health monitoring systems. Procedia Computer Science, 258, 3857-3866.

Bonina, C., Koskinen, K., Eaton, B., Gawer, A. (2021), Digital platforms for development: Foundations and research agenda. Information

Systems Journal, 31(6), 869-902.
Cenamor, J., Sjödin, D.R., Parida, V. (2017), Adopting a platform approach in servitization. International Journal of Production Economics, 192, 54-65.
Cosma, S., Rimo, G. (2024), Redefining insurance through technology. Research in International Business and Finance, 70, 102301.
Da Silva Faia, V., Vieira, V.A. (2018), Moderating effects in regression analysis. Brazilian Journal of Management, 11(4), 961-979.
Dong, P., Quan, Z., Edwards, B., Wang, S., Feng, R., Wang, T., Foley, P., Shah, P. (2024), Privacy-Enhancing Collaborative Information Sharing Through Federated Learning: Evidence from Insurance Industry; [arXiv Preprint].
Elgargouh, Y., Reda, M., Zemmouri, E.M., Behja, H. (2024), Knowledge management for digital transformation in insurance. Informatics, 11(3), 60.
Faqih, R., Nurhayati, N. (2023), Opportunities and challenges of FinTech in takaful services. El-Buhuth Borneo Journal of Islamic Studies, 5(2), 231-243.
Gazali, H.M., Haque, M.M., Shafiai, S., Shamsudin, N., Mohd, S. (2023), Conceptual Insights on Factors Shaping Takaful Technology (Takatech) Adoption in Malaysia. Malaysia: UMS Institutional Repository.
Gold, A.H., Malhotra, A., Segars, A.H. (2001), Knowledge management capabilities. Journal of Management Information Systems, 18(1), 185-214.
Hamid, Z., Khalique, F., Mahmood, S. (2024), Healthcare insurance fraud detection using data mining. BMC Medical Informatics and Decision Making, 24, 112.
Hassan, M.S., Islam, M.A., Mohd, Nasir, H. (2023), Users' fintech services acceptance: A cross-sectional study on Malaysian insurance and takaful industry. Heliyon, 9(11), e21130.
Hassan, R., Salman, S.A., Kassim, S., Majdi, H. (2018), Awareness and knowledge of takaful in Malaysia: A survey of Malaysian consumers. International Journal of Business and Social Science, 9(11), 45-53.
Helfat, C.E., Raubitschek, R.S. (2018), Dynamic and integrative capabilities in digital platform ecosystems. Research Policy, 47(8), 1391-1399.
Hellemans, I., Porter, A.J., Diriker, D. (2021), Digital platforms for sustainable development. Business Strategy and the Environment, 31(2), 668-683.
Hussain, H., Jun, W., Radulescu, M. (2025), Innovation performance in digital divide context. Journal of Knowledge Economy, 16(1), 3772-3792.
Kasim, N., Nu, S., Salman, S.A. (2015), Risk-sharing and shared prosperity through takaful. Middle East Journal of Scientific Research, 23(11), 2713-2721.
Kazan, E., Tan, C.W., Lim, E.T.K., Sørensen, C., Damsgaard, J. (2018), Digital platform competition. Journal of Management Information Systems, 35(1), 180-219.
Kondapaka, K.K. (2021), AI-driven solutions for fraud detection and prevention in insurance: Advanced techniques and applications. International Journal of Computer Science and Information Technology Research, 9(2), 45-56.
Kurdi, O.F.A. (2024), Online research collaboration platforms for knowledge sharing. International Journal of Business Innovation and Research, 33(4), 433-456.
Malhotra, N.K., Kim, S.S., Agarwal, J. (2004), Internet users' information privacy concerns: The construct, the scale, and a causal model. Information Systems Research, 15(4), 336-355.
Mehboob, I., Arijo, S., Noordin, K., Karsing, N., Amin, H. (2025), Integrating technology self-efficacy, perceived social security, and halal product image with the DOI model: Evidence from takaful in Sabah, Malaysia. Journal of Islamic Marketing, ahead-of-print. ahead-of-print. https://doi.org/10.1108/JIMA-06-2024-0247.
Memon, U., Waseem, M., Abidin, M.Z.U., Junejo, Z., Ali, M. (2024), Turning crisis into opportunity: The emergence of cyber risk takaful in the digital world. Emerald Emerging Markets Case Studies, 14(3), 1-24.
Mohy-Ul-Din, S., Samad, S., Rehman, M.A., Ali, M.Z., Ahmad, U. (2019), Trust and expertise in takaful services. International Journal of Islamic and Middle Eastern Finance and Management, 12(4), 509-522.
Nugroho, R.A., Apriantoro, M.S. (2025), Digital discourses on takaful: Public perception via social network analysis. I-iECONS e-Proceedings, 11(1), 520-533.
Parhi, P., Debata, P.P., Bisi, S.K., Behera, A.A., Sahoo, B.K., Kumar, R., Solanki, V., Lamba, V. (2025), Blockchain-based knowledge management systems. IET Conference Proceedings, 2024(23), 28-33.
Preacher, K.J., Hayes, A.F. (2008), Indirect effects in multiple mediator models. Behavior Research Methods, 40(3), 879-891.
Rai, A., Tang, X. (2010), Leveraging IT capabilities for interorganizational relationships. Information Systems Research, 21(3), 516-542.
Ramachandaran, S., Mahalley, Z., Nuraini, R., Dhar, B.K. (2025), Challenges of AI-driven business intelligence systems in the Malaysian insurance industry. F1000Research, 14, 452.
Singh, R.M., Gupta, M. (2014), Knowledge management in teams: Empirical integration and development of a scale. Journal of Knowledge Management, 18(4), 777-794.
Smith, J.H., Milberg, S.J., Burke, S.J. (1996), Information privacy: Measuring individuals' concerns. MIS Quarterly, 20(2), 167-196.
Stewart, K.A., Segars, A.H. (2002), Concern for information privacy instrument. Information Systems Research, 13(1), 36-49.
Tambi, M.R., Rahman, A. (2023), Digital platform ecosystem for insurance investment industry in Malaysia: A conceptual solution. Journal of Information Systems and Digital Transformation, 5(1), 101-112.
Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D. (2003), User acceptance of information technology. MIS Quarterly, 27(3), 425-478.
Vuković, D.B., Dekpo-Adza, S., Matović, S. (2025), AI integration in financial services: Trends and regulatory challenges. Humanities and Social Sciences Communications, 12(1), 562.
Wahyuni, E.T. (2022), Digital transformation and IFRS 17 accounting issues in takaful industry: The case of Indonesia. In: Digital Transformation in Islamic Finance. London, UK: Routledge, p218-234.
Williamson, B. (2021), Making markets through digital platforms. Critical Studies in Education, 62(1), 50-66.
Ximei, L., Latif, Z., Danish, Latif, S., Waraa, K.U. (2022), Estimating the impact of information technology on economic growth in South Asian countries: The silver lining of education. Information Development, 40(1), 147-157.
Zhang, Z., Zou, Y., Guo, B.H.W., Dimyadi, J., Davies, R., Jiang, L. (2024), Knowledge management for off-site construction. Automation in Construction, 166, 105632.