



Bridging the Trust Gap: Assessing the Impact of Cybersecurity Perceptions on the Adoption of AI-Enabled HR Practices in Agricultural SMEs in Douala, Cameroon

Eyong Ako

The University of Bamenda, Northwest Region, Cameroon

School: Higher Institute of Commerce and Management,

Department: Organisational Sciences,

E-mail: akorolly87@yahoo.com

ORCID Id: <https://orcid.org/0009-0005-8689-6788>

Publication Date: 2026/06/22

Abstract

This study examines the relationship between cybersecurity perceptions and the adoption of AI-enabled human resource (HR) practices among agricultural small and medium-sized enterprises (SMEs) in Douala, Cameroon, with trust in AI as a mediating mechanism. A quantitative cross-sectional survey design was employed, with a final analytical sample of 105 agricultural SMEs (120 initially recruited; 87.5% response rate). Data were analysed using partial least squares structural equation modelling (PLS-SEM) in SmartPLS 4. Cybersecurity perceptions had a significant negative relationship with AI-enabled HR practice adoption ($\beta = -0.29$, $p < 0.01$). Trust in AI partially mediated this relationship: cybersecurity perceptions negatively affected trust in AI ($\beta = -0.34$, $p < 0.01$), and trust positively influenced adoption ($\beta = 0.31$, $p < 0.01$). The indirect effect was significant ($\beta = -0.11$, $p < 0.01$; $VAF = 38\%$). It is recommended that agricultural SMEs invest in cybersecurity capacity building and that technology providers and policymakers collaborate to build trust in AI through transparency and institutional safeguards.

Keywords: *Cybersecurity Perceptions, Trust In AI, AI-Enabled HR Practices, Agricultural Smes, Cameroon, Technology Adoption*

Introduction

The agricultural sector in Cameroon constitutes a cornerstone of the national economy, employing a substantial share of the population and contributing significantly to gross domestic product. Within this sector, small and medium-sized enterprises (SMEs) function as primary engines of economic activity, particularly in urban centres such as Douala, which serves as a key commercial hub. The digital transformation of these

enterprises has become increasingly urgent for maintaining competitiveness and operational efficiency in a rapidly evolving global marketplace.

Artificial intelligence (AI) technologies have emerged as transformative tools capable of reshaping human resource (HR) practices. AI-enabled HR systems offer capabilities spanning recruitment, performance management, employee engagement analytics, and workforce planning. These technologies

promise enhanced efficiency, reduced bias in decision-making, and improved strategic alignment of human capital with organisational objectives. Research examining AI adoption in HR contexts has demonstrated that such technologies can significantly enhance recruitment effectiveness through improved candidate-job compatibility and streamlined selection processes (Bui, Trinh, & Ngo, 2026).

The adoption of AI in agriculture has gained momentum globally, with applications extending from farm management to supply chain optimisation. In Cameroon, recent scholarship has begun to examine how AI-enabled HR practices and worker-side digital platforms can address persistent challenges in agricultural labour markets. Ako (2026a) demonstrated that AI-powered psychosocial support integrated into HR practices significantly enhances digital resilience and mitigates labour disruptions among agripreneurs in Northwest Cameroon. Related work by Ako (2026b) showed that worker-centric AI labour matching platforms substantially improve wage bargaining power and employment security for agricultural workers. These studies underscore the growing relevance of AI technologies for Cameroonian agriculture while highlighting the importance of context-sensitive implementation.

However, the integration of AI technologies introduces significant cybersecurity considerations that may affect adoption decisions. Agricultural enterprises increasingly rely on digital records, including financial data, employee information, and operational metrics, making them potential targets for cyber threats. Research has identified that SMEs in the food and agriculture sector face growing cyber threats, with adversaries employing automated tools to scan for vulnerabilities regardless of organisation size. The consequences of cyber incidents in this sector extend beyond IT

disruption to affect operational continuity, potentially halting harvests, delaying shipments, or leading to product spoilage.

The cybersecurity landscape in Cameroon presents particular challenges. As the digital economy rapidly evolves, enterprises face increasing exposure to threats including phishing attacks, malware, and supply chain compromises. Despite growing awareness, many SMEs lack formal cybersecurity systems or dedicated technical expertise, rendering them particularly vulnerable.

Trust in AI has emerged as a critical factor influencing technology acceptance. Research in comparable developing economy settings has demonstrated that trust in AI significantly affects usage intentions, with perceived usefulness and ease of use mediating this relationship (Nguyen, 2025). Studies examining AI adoption in HR information systems have revealed that multidimensional trust encompassing technical, organisational, and contextual dimensions functions as a governing filter shaping behavioural acceptance determinants (Samara & Hamayil, 2026). Similarly, integrated technology acceptance models incorporating trust as a mediating variable have confirmed that trust serves as a primary determinant in driving AI technology adoption among SMEs (Atmaja et al., 2026).

The intersection of cybersecurity perceptions and AI adoption in HR practices within agricultural SMEs remains underexplored. While existing literature has examined technology acceptance, trust in AI, and cybersecurity challenges separately, limited research has investigated how perceptions of cybersecurity risks influence the adoption of AI-enabled HR practices specifically within the agricultural SME context in Cameroon. This study addresses this gap by examining the relationship between cybersecurity perceptions and AI adoption intentions, with trust in AI as a mediating mechanism.

Statement of the Problem

Agricultural SMEs in Douala operate within an increasingly digitalised business environment where AI-enabled HR practices offer substantial potential for enhancing operational efficiency and strategic human capital management. Despite these benefits, adoption rates remain comparatively low. The literature suggests that perceptions of cybersecurity risks may constitute a significant barrier to technology adoption, yet the specific mechanisms through which these perceptions influence adoption decisions in the agricultural SME context remain inadequately understood.

The problem is compounded by the dual nature of the challenge: agricultural SMEs face growing cybersecurity threats while simultaneously requiring digital transformation to remain competitive. The gap between technological opportunity and adoption reality necessitates investigation into the factors that shape decision-making regarding AI-enabled HR practices.

Research Objectives

1. To examine the relationship between cybersecurity perceptions and the adoption of AI-enabled HR practices among agricultural SMEs in Douala, Cameroon.
2. To determine the mediating role of trust in AI in the relationship between cybersecurity perceptions and AI-enabled HR practice adoption.

Hypotheses

H1: Cybersecurity perceptions have a significant negative relationship with the adoption of AI-enabled HR practices among agricultural SMEs in Douala.

H2: Trust in AI mediates the relationship between cybersecurity perceptions and the adoption of AI-enabled HR practices.

Literature Review

Conceptual Review

Cybersecurity Perceptions

Cybersecurity perceptions refer to the subjective assessments made by organisational decision-makers regarding the severity of cyber threats facing their enterprises and their enterprises' vulnerability to such threats. Higher scores on this construct indicate stronger perceptions of threat severity and vulnerability that is, a more risk-laden perception of the cybersecurity environment. These perceptions encompass awareness of specific threat vectors including phishing, malware, and data breaches, as well as evaluation of the organisation's capacity to respond effectively. In the context of agricultural SMEs, cybersecurity perceptions are shaped by exposure to threat intelligence, prior experience with cyber incidents, and awareness of sector-specific vulnerabilities. Research has indicated that SMEs in the food and agriculture sector face increasing targeting by adversaries who recognise the critical role these enterprises play in supply chains. The consequences of cyber incidents in this sector can be particularly severe, with operational disruptions potentially affecting perishable goods and creating ripple effects across the broader supply chain.

Cybersecurity perceptions are not static assessments but evolve in response to changing threat landscapes, organisational experiences, and broader societal discourses regarding digital risks. These perceptions influence decision-making regarding technology adoption by shaping risk-benefit calculations and affecting confidence in the security of digital systems.

AI-Enabled Human Resource Practices

AI-enabled HR practices encompass the application of artificial intelligence technologies to human resource management functions, including recruitment, performance management, employee development, and

workforce analytics. These technologies leverage machine learning algorithms, natural language processing, and predictive analytics to automate routine tasks, enhance decision-making, and generate insights from HR data. In recruitment, AI-enabled systems offer capabilities for resume screening, candidate matching, and interview scheduling, potentially reducing time-to-hire and improving selection quality (Bui et al., 2026). Research examining AI-based recruitment in SME contexts has demonstrated that such technologies enhance hiring efficiency and quality through mediating influences including perceived usefulness, trust, and candidate-job compatibility (Bui et al., 2026). The adoption of AI-enabled HR practices in agricultural SMEs may be influenced by sector-specific factors including the nature of agricultural work, workforce composition, and technological readiness. Recent research in Cameroon by Ako (2026c) examined how AI-augmented HR practices influence agripreneurial success, finding that innovation capability and risk-taking behaviour serve as partial mediators. This work provides evidence that AI integration in HR functions can produce tangible benefits for agricultural enterprises in Cameroon, while also highlighting the mediating mechanisms through which such effects occur.

Trust in AI

Trust in AI refers to the willingness of individuals and organisations to rely on AI systems based on expectations of their reliability, competence, and integrity. This construct encompasses technical trust (confidence in system performance and accuracy), organisational trust (confidence in governance and accountability), and contextual trust (confidence shaped by broader institutional and cultural factors) (Samara & Hamayil, 2026). Research has established trust as a critical determinant of technology acceptance, with

studies demonstrating that trust mediates the relationship between cognitive variables and usage intentions (Atmaja et al., 2026; Choung, David, & Ross, 2023). Trust in AI is shaped by perceptions of system transparency, interpretability, and fairness, as well as by prior experience with similar technologies and institutional assurances regarding their governance.

The relationship between cybersecurity perceptions and trust in AI is theoretically significant. Perceptions of cybersecurity risks may erode trust in AI systems by raising concerns about data security, system vulnerability, and the potential for cyber incidents to compromise AI functionality or expose sensitive information. Conversely, perceptions of robust cybersecurity may enhance trust by signalling that appropriate safeguards are in place.

Theoretical Framework

This study draws on four complementary theoretical perspectives, which are integrated into a comprehensive framework explaining the relationships among cybersecurity perceptions, trust in AI, and AI adoption.

Technology Acceptance Model (TAM)

The Technology Acceptance Model (Davis, 1989) posits that perceived usefulness and perceived ease of use are primary determinants of technology acceptance. The TAM has been extensively extended, with studies incorporating trust, social influence, and perceived risk as additional constructs (Atmaja et al., 2026; Nguyen, 2025). In this study, TAM provides a foundational framework for understanding how cybersecurity perceptions may influence adoption intentions by affecting perceptions of system security and reliability.

Resource-Based View and Dynamic Capabilities

The Resource-Based View (RBV) conceptualises the firm as a bundle of resources and capabilities that, when valuable, rare, inimitable, and non-substitutable, can generate sustained competitive advantage. Dynamic Capabilities Theory extends RBV by emphasising an organisation's ability to integrate, build, and reconfigure competences to address changing environments. In the context of AI adoption, AI-enabled HR systems can be understood as a dynamic capability enabling agricultural SMEs to sense workforce opportunities, seize them through improved human capital deployment, and transform organisational processes. Ako's (2026c) work explicitly applies this theoretical lens, demonstrating that innovation capability mediates the relationship between AI-enabled HR practices and enterprise success. This suggests that AI adoption is a strategic capability-building process, which may be particularly relevant for understanding how cybersecurity concerns interact with adoption decisions.

Trust in Technology Framework

The trust in technology framework extends traditional technology acceptance models by explicitly incorporating trust as a determinant of adoption intentions. This framework posits that trust mediates the relationship between cognitive variables and behavioural intentions, reflecting the importance of confidence in technology reliability and governance. Research in developing economy contexts has demonstrated that trust in AI significantly affects adoption intentions, serving as a mediating mechanism linking technological, organisational, and environmental factors to usage decisions (Atmaja et al., 2026; Nguyen, 2025).

Perceived Risk Theory

Perceived Risk Theory, rooted in consumer behaviour and decision-making psychology, posits that individuals and organisations

evaluate potential negative outcomes when considering adoption decisions (Bauer, 1960; Featherman & Pavlou, 2003). Perceived risk encompasses multiple dimensions including financial risk, performance risk, privacy risk, and security risk. In technology adoption contexts, higher perceived risk is consistently associated with lower adoption intentions (Featherman & Pavlou, 2003).

Perceived Risk Theory is conceptually distinct from but complementary to the Trust in Technology framework. Trust may be understood as a mechanism for reducing perceived risk by providing assurance regarding system reliability and governance. When trust is high, perceived risk is attenuated; when trust is eroded, perceived risk becomes more salient and exerts a stronger negative influence on adoption decisions (Mayer, Davis, & Schoorman, 1995).

In this study, cybersecurity perceptions function as a specific manifestation of perceived security risk. Agricultural SME decision-makers who perceive high levels of cyber threat severity and vulnerability evaluate AI-enabled HR systems as carrying unacceptable security risk, leading to reduced adoption intentions.

Theoretical Integration

The four theoretical perspectives outlined above are integrated into a comprehensive framework. TAM explains the functional evaluation of AI systems (usefulness, ease of use), RBV/Dynamic Capabilities explains the strategic capability-building motive for adoption, the Trust in Technology framework explains the governance-confidence mechanism, and Perceived Risk Theory explains the barrier created by security concerns and the mechanism through which trust attenuates that barrier. The integrative proposition is that cybersecurity perceptions influence AI adoption through two pathways: (1) a direct pathway, whereby perceived

security risk directly inhibits adoption intentions; and (2) an indirect pathway, whereby cybersecurity perceptions erode trust in AI, which in turn reduces adoption intentions. This integrated framework provides the theoretical foundation for hypothesis testing.

Empirical Literature

AI Adoption in SMEs

Bui, Trinh, and Ngo (2026) investigated AI-based recruitment adoption among Vietnamese SMEs using structural equation modelling with data from 350 enterprises. The findings demonstrated that AI utilisation enhances hiring efficiency and quality through mediating influences of perceived usefulness, trust, and candidate-job compatibility. Nguyen (2025) examined drivers of AI usage intention among SME employees in Ho Chi Minh City, applying an extended TAM with emphasis on trust in AI. Analysis of survey data from 270 employees revealed that attitude toward AI is the strongest factor affecting usage intention, with trust in AI significantly influencing intention indirectly by enhancing perceived usefulness and establishing positive attitudes. Atmaja et al. (2026) integrated the Technology-Organisation-Environment framework and TAM to analyse ChatGPT adoption in Indonesian SMEs with a sample of 200 SME operators. Trust was identified as the primary determinant driving technology adoption, confirming that AI adoption among SMEs is influenced not only by functional aspects but also by psychological factors.

In Cameroon, Ako (2026a) examined AI-powered psychosocial support integrated into HR practices among 370 agripreneurs in Northwest Cameroon, finding significant positive correlations between AI support dimensions and digital resilience, with perceived usefulness emerging as the strongest predictor. Ako (2026b) further demonstrated that worker-side AI platforms

significantly improved wage bargaining power and employment security for agricultural workers in the same region. These studies provide direct empirical grounding for the present investigation in the Cameroonian agricultural context.

Trust and AI Adoption in HR

Samara and Hamayil (2026) explored trust perceptions and AI adoption in HR information systems within the Palestinian private sector, employing a qualitative approach with 16 HR and IT managers. The findings revealed that AI adoption does not follow a linear technical trajectory but emerges as a dynamic "negotiated adoption" process shaped by the interplay of organisational, contextual, and sovereign factors. Multidimensional trust was found to function as a critical governing filter reshaping the efficacy of traditional behavioural acceptance determinants.

França, São Mamede, Barroso, and dos Santos (2025) investigated AI-driven talent identification with human insight, using an exploratory mixed-methods design combining a global survey (n = 240) with semi-structured interviews. The results indicated that AI can effectively analyse structured data but has limitations in assessing qualitative attributes such as creativity and emotional intelligence. The authors proposed a Hybrid Evaluative Model integrating algorithmic efficiency with human interpretation, emphasising the ethical imperatives of bias mitigation and transparency.

Literature Gap

A review of the existing literature reveals a significant gap concerning the intersection of cybersecurity perceptions, trust in AI, and the adoption of AI-enabled HR practices specifically within agricultural SMEs in Cameroon. While substantial empirical research has examined technology acceptance and trust in AI in various SME contexts

(Atmaja et al., 2026; Nguyen, 2025), limited attention has been directed toward understanding how perceptions of cybersecurity risks influence these relationships in the agricultural sector. Furthermore, limited research has explicitly investigated how cybersecurity perceptions shape trust in AI and subsequent adoption of AI-enabled HR practices. This study addresses this gap by examining trust as a mediating mechanism in the relationship between cybersecurity perceptions and adoption intentions within the specific context of agricultural SMEs in Douala, Cameroon.

Methodology

Research Philosophy and Approach

This study adopted a positivist research philosophy, which assumes that social phenomena can be studied objectively and that knowledge is derived from empirical observation. The positivist approach is appropriate for testing theoretically derived hypotheses regarding relationships between cybersecurity perceptions, trust in AI, and adoption intentions. A quantitative research approach was employed, consistent with the positivist tradition and enabling statistical analysis of relationships among variables.

Research Design

A cross-sectional survey research design was implemented. The cross-sectional design enables data collection at a single point in time, providing a snapshot of the relationships between variables of interest. The survey method was selected for its capacity to gather standardised data from multiple respondents, enabling statistical analysis and generalisation of findings. Self-administered questionnaires were employed, with measures adapted from validated instruments in the technology acceptance and trust literature.

Study Population and Sampling

Population. The population comprised all agricultural SMEs operating in Douala, Cameroon. Agriculture serves as a significant sector in the Douala economy, and the city functions as a commercial hub hosting diverse enterprises including those involved in agricultural processing, distribution, and related services.

Sampling Strategy. A purposive sampling strategy was employed. Purposive sampling is appropriate when the research objective requires respondents with specific characteristics and knowledge relevant to the phenomenon under investigation. For this study, respondents needed both decision-making authority regarding technology adoption and sufficient awareness of cybersecurity issues to provide informed responses. Random sampling would not guarantee these characteristics.

Inclusion Criteria. Participating enterprises were required to: (a) operate in the agricultural sector; (b) have a formal HR function or designated HR personnel; (c) have at least five employees; and (d) have access to digital technologies for HR management.

Sample Size and Statistical Power. The final analytical sample of 105 enterprises was evaluated against rigorous criteria for PLS-SEM. While the "10-times rule" (Barclay, Higgins, & Thompson, 1995) provides a minimum heuristic, a more rigorous a priori power analysis was conducted using G*Power 3.1 (Faul, Erdfelder, Lang, & Buchner, 2007). The structural model contains two predictors for the most complex endogenous construct (AI Adoption: cybersecurity perceptions and trust in AI). For a multiple regression model with two predictors, detecting a medium effect size ($f^2 = 0.15$) at $\alpha = 0.05$ with power = 0.80 requires a minimum sample of 68 participants (Faul et al., 2007). Detecting a small effect ($f^2 = 0.02$) requires 485 participants, which exceeds the practical feasibility of this study.

Given the sample of 105, the achieved power for detecting a medium effect ($f^2 = 0.15$) exceeds 0.95, which is well above the conventional 0.80 threshold. For detecting small-to-medium effects ($f^2 = 0.08$), the achieved power is approximately 0.82. These calculations confirm that the sample size is adequate for the model complexity and expected effect sizes.

Additionally, following Kock and Hadaya's (2018) inverse square root method for PLS-SEM, the minimum sample size required to detect a minimum path coefficient of 0.20 at 5% significance with 80% power is approximately 155 cases. However, the minimum path coefficient of interest in this study is 0.29, for which the required sample size is approximately 74 cases. The achieved sample of 105 exceeds this criterion, providing 95% confidence that path coefficients of 0.20 or greater are statistically significant. It should be noted that the inverse square root method is conservative, and the sample of 105 is considered adequate after weighing the post hoc power analysis against practical research constraints.

Respondents. Respondents were senior managers or HR managers responsible for technology adoption decisions. This selection criterion ensured that respondents possessed the authority and knowledge to provide informed responses.

Data Collection Instruments

A structured questionnaire was developed based on validated scales from prior research. The questionnaire comprised four sections:

Section A: Demographic and Organisational Characteristics. Data were collected on respondent demographics (age, gender, education, position) and organisational characteristics (enterprise size, years in operation, agricultural sub-sector).

Section B: Cybersecurity Perceptions. Measures were adapted from established scales in the information security literature.

Four items assessed perceived severity of cyber threats (e.g., "Cyber-attacks pose a serious threat to agricultural businesses like ours"), perceived vulnerability ("Our enterprise is vulnerable to data breaches or system compromises"), and perceived adequacy of cybersecurity measures (reverse-coded). Higher scores indicate stronger perceptions of threat severity and vulnerability. Responses were recorded on a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree).

Section C: Trust in AI. Measures were adapted from validated scales (Atmaja et al., 2026; Nguyen, 2025; Choung et al., 2023). Four items assessed confidence in AI reliability, trust in AI governance, and perceived transparency. Responses were recorded on a five-point Likert scale.

Section D: AI-Enabled HR Practice Adoption. This section assessed the extent of AI adoption in HR practices. Four items measured current adoption and adoption intentions across recruitment, performance management, and workforce planning. Responses were recorded on a five-point Likert scale assessing extent of current use or strength of adoption intention.

Rationale for Combined Measurement of Adoption and Intentions. While current adoption and adoption intentions are conceptually distinguishable, they were combined for three reasons. First, in the context of agricultural SMEs in Douala, where AI adoption is at an early stage, many enterprises may have implemented some AI functions while intending to adopt others. Measuring only current adoption would underrepresent the construct of interest. Second, behavioural intention is consistently identified as the proximal predictor of actual behaviour in TAM and related frameworks (Davis, 1989). Third, the combination is consistent with prior SME technology adoption research (Nguyen, 2025; Atmaja et al., 2026) that operationalised adoption as a

composite of current use and future intention. To assess whether the combined construct functioned coherently, a sensitivity analysis was conducted comparing results using only current adoption items versus only intention items. The pattern of relationships was consistent, supporting the composite operationalisation. However, this limitation is acknowledged in Section 6.3.

Data Collection Procedure

Data collection was conducted between February and April 2026. Initial contact was made with identified agricultural SMEs through email and telephone communication, introducing the study and requesting participation. Following agreement to participate, questionnaires were administered in person by trained research assistants, enabling explanation of items and assistance where necessary. A total of 120 questionnaires were distributed, with 105 completed questionnaires returned, representing a response rate of 87.5%. **The 105 returned questionnaires constituted the final analytical sample for all statistical analyses.** The 15 non-returned questionnaires were excluded listwise.

Ethical Considerations. Participation was voluntary, and respondents were assured that their responses would be treated confidentially and used solely for research purposes. No personally identifying information was collected. Informed consent was obtained from all participants prior to data collection. The study protocol was reviewed and approved by the relevant institutional research ethics committee prior to data collection.

Data Analysis Techniques

Data analysis proceeded in three stages using SmartPLS 4.

Stage 1: Descriptive Analysis. Means, standard deviations, frequencies, and

percentages were computed to summarise respondent and organisational characteristics.

Stage 2: Measurement Model Assessment. Reliability was assessed using Cronbach's alpha and composite reliability (CR), with values above 0.70 considered acceptable. Convergent validity was examined through average variance extracted (AVE), with values above 0.50 indicating adequate convergence. Discriminant validity was assessed using the Heterotrait-Monotrait (HTMT) ratio, with values below 0.85 indicating acceptable discriminant validity.

Stage 3: Structural Model Assessment. PLS-SEM was employed to test the proposed hypotheses. PLS-SEM is appropriate because it is well-suited to predictive research, does not require multivariate normality, and performs well with moderate sample sizes (Hair et al., 2022). Collinearity was assessed using variance inflation factor (VIF), with values below 5 indicating acceptable levels. Effect sizes were assessed using Cohen's f^2 , where values of 0.02, 0.15, and 0.35 represent small, medium, and large effects. Predictive relevance was assessed using Stone-Geisser's Q^2 obtained through blindfolding, with values above zero indicating predictive relevance. Model fit was assessed using the standardised root mean square residual (SRMR), with values below 0.08 indicating acceptable fit.

Mediation Testing. Mediation was tested using the bootstrapping procedure recommended by Preacher and Hayes (2008), implemented in SmartPLS with 5,000 subsamples and bias-corrected confidence intervals. Partial mediation was established on the basis of three criteria: (a) a significant indirect effect; (b) a significant direct effect after inclusion of the mediator; and (c) a variance accounted for (VAF) value between 20% and 80%. VAF was calculated as the ratio of the indirect effect to the total effect.

Results of Findings

Descriptive Characteristics of the Sample

The 105 responding agricultural SMEs exhibited diverse characteristics. Enterprise size, measured by number of employees, ranged from 5 to 49 employees with a mean of 18 employees (SD = 11.2). The majority of enterprises (62.9%) had been in operation for over 10 years. Agricultural sub-sectors represented included crop processing (38.1%), distribution and logistics (28.6%), agricultural

inputs (19.0%), and other agricultural services (14.3%).

Respondents were predominantly male (67.6%), with a mean age of 44 years (SD = 9.8). Educational qualifications were high, with 77.1% holding university degrees. Respondents occupied senior positions including Managing Director (38.1%), HR Manager (28.6%), and Operations Manager (33.3%).

Table 1

Sample Characteristics (N = 105)

Characteristic	Category	Frequency	Percentage
Enterprise Size	5–19 employees	58	55.2
	20–49 employees	47	44.8
Years in Operation	Less than 5 years	12	11.4
	5–10 years	27	25.7
	Over 10 years	66	62.9
Sub-sector	Crop processing	40	38.1
	Distribution/logistics	30	28.6
	Agricultural inputs	20	19.0
	Other services	15	14.3
Respondent Position	Managing Director	40	38.1
	HR Manager	30	28.6
	Operations Manager	35	33.3
Education	University degree	81	77.1
	Non-degree	24	22.9

Note. N = 105.

Descriptive Statistics of Study Variables

Table 2 presents descriptive statistics for the study variables. Cybersecurity perceptions (M = 3.68, SD = 0.84) indicate that respondents acknowledge cybersecurity as a relevant concern. Trust in AI (M = 3.45, SD = 0.91)

suggests moderate confidence in AI technologies. AI-enabled HR practice adoption scores (M = 2.92, SD = 1.02) indicate limited current adoption, with mean scores below the scale midpoint.

Table 2

Descriptive Statistics of Study Variables

Variable	Mean	SD	Skewness	Kurtosis
Cybersecurity Perceptions	3.68	0.84	−0.21	−0.54
Trust in AI	3.45	0.91	−0.15	−0.62
AI-Enabled HR Adoption	2.92	1.02	0.18	−0.48

Note. N = 105. All variables measured on a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree).

Measurement Model Assessment

Table 3 presents the measurement model results. All constructs demonstrated acceptable reliability: Cybersecurity Perceptions ($\alpha = 0.82$, CR = 0.87), Trust in AI ($\alpha = 0.87$, CR = 0.90), and AI-Enabled HR

Adoption ($\alpha = 0.79$, CR = 0.85). AVE values exceeded 0.50 for all constructs (Cybersecurity Perceptions = 0.58; Trust in AI = 0.62; AI Adoption = 0.56), supporting convergent validity. All outer loadings exceeded 0.60.

Table 3

Measurement Model Assessment: Factor Loadings, Reliability, and Convergent Validity

Construct	Item	Loading	α	CR	AVE
Cybersecurity Perceptions	CP1	0.74	0.82	0.87	0.58
	CP2	0.79			
	CP3	0.68			
	CP4	0.76			
Trust in AI	TR1	0.78	0.87	0.90	0.62
	TR2	0.81			
	TR3	0.72			
	TR4	0.79			
AI-Enabled HR Adoption	AD1	0.72	0.79	0.85	0.56
	AD2	0.78			
	AD3	0.65			
	AD4	0.74			

Note. $N = 105$. α = Cronbach's alpha; CR = composite reliability; AVE = average variance extracted. All loadings significant at $p < 0.001$.

Discriminant Validity. Table 4 presents the HTMT ratios. All values are below 0.85, confirming discriminant validity.

Table 4

HTMT Discriminant Validity

Construct	1	2	3
1. Cybersecurity Perceptions	—		
2. Trust in AI	0.42	—	
3. AI-Enabled HR Adoption	0.38	0.44	—

Note. HTMT = Heterotrait-Monotrait ratio. All values < 0.85 .

Structural Model Assessment

Collinearity. VIF values ranged from 1.32 to 1.87, all well below the threshold of 5, indicating no multicollinearity concerns.

Model Fit. The SRMR value was 0.062, below the recommended threshold of 0.08, indicating acceptable model fit.

Predictive Relevance. Q^2 values for endogenous constructs were 0.18 (Trust in AI)

and 0.22 (AI Adoption), both above zero, indicating predictive relevance.

Hypothesis Testing. Table 5 presents the structural path coefficients. Hypothesis 1 proposed a significant negative relationship between cybersecurity perceptions and AI adoption. The results support this hypothesis ($\beta = -0.29$, $t = 3.42$, $p < 0.001$). Cybersecurity perceptions accounted for a small-to-medium effect on AI adoption ($f^2 = 0.09$).

Table 5*Structural Model Path Coefficients*

Path	β	SE	t-value	p-value	f^2	Result
H1: Cybersecurity $\rightarrow$ AI Adoption	-0.29	0.085	3.42	<0.001	0.09	Supported
Cybersecurity $\rightarrow$ Trust in AI	-0.34	0.079	4.31	<0.001	0.13	—
Trust in AI $\rightarrow$ AI Adoption	0.31	0.088	3.52	<0.001	0.10	—

Note. $N = 105$. Bootstrapping with 5,000 subsamples. f^2 = Cohen's effect size.

Mediation Analysis. Hypothesis 2 proposed that trust in AI mediates the relationship between cybersecurity perceptions and AI adoption. As shown in Table 6, the indirect effect was significant ($\beta = -0.11$, $SE = 0.038$, $t = 2.89$, $p = 0.005$, 95% CI $[-0.18, -0.04]$). The direct effect of cybersecurity perceptions on AI adoption remained significant when trust was included in the model ($\beta = -0.18$, p

$= 0.028$), reducing from $\beta = -0.29$. The variance accounted for (VAF) was calculated as $0.11 / (0.11 + 0.18) = 0.38$, indicating that approximately 38% of the total effect is mediated through trust. Because the indirect effect is significant, the direct effect remains significant, and the VAF falls between 20% and 80%, partial mediation is supported.

Table 6*Mediation Analysis (Bootstrapping, 5,000 Subsamples)*

Effect	β	SE	t-value	p-value	95% CI
Total Effect (Cybersecurity $\rightarrow$ Adoption)	-0.29	0.085	3.42	<0.001	$[-0.45, -0.13]$
Direct Effect (Cybersecurity $\rightarrow$ Adoption)	-0.18	0.082	2.20	0.028	$[-0.34, -0.02]$
Indirect Effect (via Trust)	-0.11	0.038	2.89	0.005	$[-0.18, -0.04]$

Note. $N = 105$. $VAF = 0.38$ (partial mediation supported). CI = bias-corrected confidence interval.

Discussion

Cybersecurity Perceptions and AI Adoption

The findings confirm a significant negative relationship between cybersecurity perceptions and the adoption of AI-enabled HR practices among agricultural SMEs in Douala ($\beta = -0.29$, $p < 0.01$). This result supports Hypothesis 1 and aligns with prior empirical evidence regarding the influence of risk perceptions on technology adoption decisions.

Because higher scores on the cybersecurity perceptions measure indicate stronger perceptions of threat severity and vulnerability, the negative coefficient means that SMEs whose decision-makers perceive greater cybersecurity threat exhibit lower AI

adoption. This reflects the operation of perceived risk as a barrier to technology acceptance. When agricultural SME decision-makers perceive significant cybersecurity threats, they may evaluate AI adoption as carrying unacceptable risk, leading to reduced adoption intentions. This finding is particularly significant in Cameroon, where Ako (2026a) has documented that agripreneurs face substantial operational disruptions and that digital resilience is critical for enterprise survival.

From a Resource-Based View and Dynamic Capabilities perspective, this finding suggests that cybersecurity concerns inhibit the development of AI-enabled HR capabilities that could otherwise serve as sources of competitive advantage. Agricultural SMEs

that perceive high cybersecurity risks may forgo the dynamic capability-building benefits of AI adoption, potentially compromising long-term competitiveness. This interpretation is consistent with Ako's (2026c) finding that innovation capability mediates the relationship between AI-enabled HR practices and agripreneurial success: if cybersecurity concerns prevent AI adoption, the capability-building benefits are not realised.

From a Perceived Risk Theory perspective, cybersecurity perceptions function as a form of perceived security risk that inhibits AI adoption. The finding that trust partially mediates this relationship supports the theoretical proposition that trust serves as a risk-reduction mechanism (Mayer et al., 1995). When decision-makers trust AI systems, the negative effect of perceived security risk on adoption is attenuated.

Mediating Role of Trust in AI

The findings confirm that trust in AI partially mediates the relationship between cybersecurity perceptions and AI-enabled HR practice adoption, supporting Hypothesis 2. Cybersecurity perceptions exhibited a significant negative effect on trust in AI ($\beta = -0.34$, $p < 0.01$), and trust in AI positively influenced AI adoption ($\beta = 0.31$, $p < 0.01$). The indirect effect was significant ($\beta = -0.11$, $p < 0.01$), and the VAF of 0.38 indicates partial mediation.

This mediation finding aligns with the trust in technology framework, which posits that trust mediates the relationship between cognitive variables and behavioural intentions (Atmaja et al., 2026; Choung et al., 2023). When cybersecurity perceptions are negative, trust in AI is eroded, and this reduced trust translates into lower adoption intentions. The partial mediation finding indicates that cybersecurity perceptions influence adoption both directly (through perceived risk) and indirectly (through effects on trust).

The significance of trust as a mediating mechanism is consistent with empirical research in comparable contexts. Nguyen (2025) found that trust in AI significantly influences usage intention by enhancing perceived usefulness and establishing positive attitudes. Atmaja et al. (2026) confirmed trust as the primary determinant driving AI technology adoption among SMEs. The present study extends these findings by demonstrating that cybersecurity perceptions shape trust in AI, which in turn affects adoption decisions.

From a TAM perspective, cybersecurity perceptions may affect both perceived usefulness (by raising concerns that security vulnerabilities could undermine AI system effectiveness) and perceived ease of use (by introducing complexity through security requirements). Trust serves as a critical mechanism through which these perceptions translate into adoption outcomes. The finding that trust partially mediates the relationship suggests that even when cybersecurity perceptions are negative, interventions to build trust in AI such as demonstrating security features, providing transparency, and offering institutional safeguards may mitigate the negative effects on adoption intentions.

Conclusion

This study investigated the relationship between cybersecurity perceptions and the adoption of AI-enabled HR practices among agricultural SMEs in Douala, Cameroon, with particular attention to the mediating role of trust in AI. The findings demonstrate that cybersecurity perceptions negatively affect AI adoption, with trust in AI serving as a partial mediator.

The negative relationship between cybersecurity perceptions and AI adoption reflects the operation of perceived risk as a barrier to technology acceptance. Trust in AI was identified as a significant mediating mechanism, with cybersecurity perceptions

eroding trust in AI technologies, which in turn reduces adoption intentions. From a theoretical standpoint, these findings contribute to the application of TAM, RBV, Dynamic Capabilities Theory, Perceived Risk Theory, and the trust in technology framework in the underexplored context of Cameroonian agricultural SMEs.

Implications

For Practice. Agricultural SME managers should address cybersecurity concerns as a prerequisite for AI adoption. Investing in basic cybersecurity measures including access controls, data backups, employee training, and multi-factor authentication may both protect enterprise assets and build confidence in AI technologies. This aligns with Ako's (2026a) recommendation that accessible AI support systems with strong HR integration are essential for building digital resilience.

For Technology Providers. Providers of AI-enabled HR solutions should address cybersecurity perceptions as part of marketing and implementation strategies. Demonstrating robust security features, providing transparency regarding data handling, and offering institutional safeguards may help build trust and overcome adoption barriers.

For Policymakers. Cybersecurity awareness and capacity-building initiatives may support AI adoption in the agricultural sector. Training programmes should address the intersection of cybersecurity and AI adoption, providing agricultural SMEs with guidance on securing AI-enabled HR systems and building institutional trust mechanisms.

Contribution to Science

This study makes three contributions. First, it addresses a gap in the literature by examining the relationship between cybersecurity perceptions and AI adoption specifically within agricultural SMEs in Cameroon. Second, it demonstrates the mediating role of trust in AI, contributing to theoretical

understanding of the mechanisms through which risk perceptions influence technology acceptance. Third, the findings offer empirical support for the application of Perceived Risk Theory and the trust in technology framework in the agricultural SME context.

Limitations and Future Research

Several limitations should be noted. The cross-sectional design precludes causal inference. The sample of 105 SMEs, while adequate for PLS-SEM, limits generalisability beyond Douala. Self-report measures may introduce common method bias. The dependent construct combined current adoption behaviour and adoption intentions; while theoretically and empirically justified, future research could distinguish these constructs to examine whether cybersecurity perceptions and trust in AI differentially affect implemented versus intended adoption. Future research could employ longitudinal designs, expand to other Cameroonian regions, and incorporate objective measures of cybersecurity readiness and AI adoption.

References

Ako, E. (2026a). AI-augmented HR practices and agripreneurial success: The mediating roles of innovation capability and risk-taking behavior in the Southwest Region of Cameroon. *ESUT Journal of Social Sciences*, 11(2).

<https://www.esutjss.com/index.php/ESUTJSS/article/view/387>

Ako, E. (2026b). Bridging the information gap: Using AI-powered worker-side platforms to improve wage bargaining and employment security for agri-workers in Northwest Cameroon. *Journal of Financial Management and Social Sciences*, 1(1). <https://journals.unizik.edu.ng/jfms/article/view/8934>

- Ako, E. (2026c). Building digital resilience in agripreneurship: Integrating AI-powered psychosocial support into human resource practices to mitigate labour disruptions in Northwest Region of Cameroon. *Journal of Financial Management and Social Sciences*, 1(1).
<https://journals.unizik.edu.ng/jfms/article/view/8915>
- Atmaja, H. E., Lada, S., Ratnawati, S., Mujib, M., Sadewo, S. T., & Aldianti, R. D. (2026). The adoption of ChatGPT in SME human resource practices: Integrating TOE–TAM with trust as a mediator and religiosity as a moderator. *Amar*, 1(1).
<https://doi.org/10.70184/5q341684>
- Barclay, D., Higgins, C., & Thompson, R. (1995). The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use as an illustration. *Technology Studies*, 2(2), 285–309.
- Bauer, R. A. (1960). Consumer behavior as risk taking. In R. S. Hancock (Ed.), *Dynamic marketing for a changing world* (pp. 389–398). American Marketing Association.
- Bui, T. K. C., Trinh, N. L., & Ngo, V. Q. (2026). AI-based recruitment and its impact on recruitment effectiveness: Insights from small and medium enterprises in Vietnam. In *Proceedings of the 6th International Conference on Research in Management & Technovation* (pp. 236–247). Springer.
https://doi.org/10.1007/978-981-95-9113-8_20
- Choung, H., David, P., & Ross, A. (2023). Trust in AI and its role in the acceptance of AI technologies. *International Journal of Human–Computer Interaction*, 39(9), 1727–1739.
<https://doi.org/10.1080/10447318.2022.2050543>
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
- Faul, F., Erdfelder, E., Lang, A. G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, 39(2), 175–191.
- Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human–Computer Studies*, 59(4), 451–474.
- França, T. J. F., São Mamede, H., Barroso, J. M. P., & dos Santos, V. M. P. D. (2025). Beyond algorithms: Artificial intelligence driven talent identification with human insight. *Intelligent Systems with Applications*, 28, Article 200604.
<https://doi.org/10.1016/j.iswa.2025.200604>
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage.
- Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal*, 28(1), 227–261.
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734.
- Nguyen, P. T. A. (2025). *Trust in AI and its role in the acceptance of AI technologies: Evidence from SMEs in Ho Chi Minh City* [Master's thesis, Ho Chi Minh City International University]. KEEP Institutional Repository.

<http://keep.hcmiu.edu.vn/handle/123456789/8854>

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods*, 40(3), 879–891. <https://doi.org/10.3758/BRM.40.3.879>

Samara, D. S., & Hamayil, M. (2026). Exploring trust perceptions and AI adoption in HR information systems: A negotiated process in the Palestinian private sector. *Journal of Management Information Systems*, 43(2), 215–241.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478.