

AI-DRIVEN CODING, MACHINE LEARNING FRAUD DETECTION, AND BLOCKCHAIN-ENABLED API INTEGRATION FOR SECURE PAYMENT GATEWAY PERFORMANCE

Thaingar Aung Soe ¹
Arkar Htet
Yu Thwe

Received 07.07.2026.
Revised 04.09.2026.
Accepted 15.10.2026.

Keywords:

AI-driven coding, machine learning fraud detection, blockchain, API integration reliability, secure payment gateways, cybersecurity resilience.

Original research



ABSTRACT

Secure digital payment gateways increasingly depend on AI-assisted development, machine-learning fraud detection, blockchain controls, and reliable system integration. This study examines how these capabilities and related operational mechanisms influence secure payment gateway performance. A cross-sectional survey of 500 technical respondents in Myanmar was analyzed using SPSS and AMOS through reliability analysis, confirmatory factor analysis, structural equation modeling, bootstrapped mediation, and moderation analysis. The measurement model showed acceptable fit ($CMIN/DF = 1.063$, $CFI = 0.993$, $RMSEA = 0.011$), and the structural model explained 64.6% of performance variance. AI-driven coding, machine-learning fraud detection, API integration reliability, security assurance quality, and blockchain trust mechanisms had significant positive direct effects, with security assurance quality showing the strongest effect. Eleven indirect effects and three moderation effects were supported. The findings highlight the importance of combining technological resources with assurance, integration, compliance, and trust capabilities to support reliable and secure digital payment services.

© 2026 Journal of Trends and Challenges in Artificial Intelligence

1. INTRODUCTION

Digital payment gateways are core infrastructure for e-commerce, banking applications, and fintech services because they must process transactions efficiently while preserving confidentiality, integrity, availability, traceability, and user trust (Aljaradat et al., 2024; Gomber et al., 2017). As digital payment adoption expands, cybersecurity and operational resilience become increasingly important because security failures

can affect service continuity, user confidence, and continued adoption (Aljaradat et al., 2024).

Artificial intelligence and machine learning are increasingly embedded in software development and financial security workflows. AI-assisted coding can accelerate prototyping, code completion, and review, while machine-learning methods can identify abnormal transaction patterns at scales that are difficult to manage manually (Dwivedi et al., 2021). However, AI-generated code requires validation: empirical studies have shown

¹ Corresponding author: Thaingar Aung Soe
Email: thaingaras@gmail.com

that code assistants can introduce security weaknesses, and recent work continues to identify trade-offs between correctness, maintainability, and security in generated code (Black et al., 2024; Perry et al., 2023). Fraud detection therefore remains a complementary capability rather than a substitute for secure software engineering. Established and recent studies show that machine-learning approaches can improve fraud identification, particularly when high-volume and imbalanced transaction data are involved (Abdallah et al., 2016; Ingle et al., 2025; Jurgovsky et al., 2018).

Blockchain-based controls offer a different security mechanism through tamper-resistant records, distributed verification, and traceability (Casino et al., 2019). Recent payment-gateway research demonstrates how blockchain and distributed storage can strengthen transaction-record integrity (Fachrian et al., 2024). At the same time, blockchain should not be treated as inherently sustainable: its environmental and energy implications depend on architecture, platform, and consensus design (Mulligan et al., 2024; Sai & Vranken, 2024). This distinction is important in sustainable-computing research because trustworthy and resilient digital infrastructure can support sustainable digital services, while environmental sustainability requires direct evidence on energy, computation, and emissions.

Cybersecurity itself is also increasingly discussed as part of sustainable digital development. Recent studies link cybersecurity to long-term organizational and infrastructure sustainability and emphasize the need to balance resilience, resource use, and environmental responsibility (Achuthan et al., 2025; Morales-Sáenz et al., 2024). Accordingly, this study treats sustainability as a contextual implication of reliable and secure digital infrastructure rather than as a directly measured environmental outcome.

1.1. Research gap and objectives

Prior research commonly examines AI-assisted development, fraud analytics, blockchain implementation, API reliability, compliance, and payment-service security as separate topics. There is less empirical evidence on how these capabilities operate together within a single payment-gateway performance model, particularly through intermediate mechanisms such as API integration reliability, compliance, security assurance, and blockchain trust. The present study addresses this gap by testing direct effects, multiple mediated pathways, and selected moderation effects in one covariance-based structural equation model.

The objectives are to:

- (1) examine the direct effects of AIC, MLF, BSC, DCQ, AIR, PGC, SAQ, and BTM on PGP;
- (2) test whether AIR, PGC, SAQ, BTM, and DCQ mediate selected technology-performance relationships;
- (3) examine moderation involving BTM and SAQ; and
- (4) evaluate the reliability, validity, and explanatory performance of the proposed model

2. LITERATURE REVIEW

2.1. Theoretical foundation

The model follows a technology-capability-performance logic. AIC, MLF, and BSC represent technology resources; DCQ, AIR, PGC, SAQ, and BTM represent operational and security mechanisms through which those resources may be converted into reliable service outcomes; and PGP represents the final system-performance outcome. This framing does not claim a single grand theory. Instead, it specifies a process logic in which technologies create value when they are converted into dependable integration, governance, assurance, and trust capabilities. BTM and SAQ are additionally examined as contextual conditions that may strengthen selected technology-performance relationships (Kshetri, 2017).

2.2. AI-driven coding

AI-driven coding refers to the use of intelligent coding assistants and automated development tools to generate, complete, explain, review, or suggest source code (Allamanis et al., 2018; Li et al., 2022; Nguyen & Nadi, 2022; Vaithilingam et al., 2022). In payment-gateway development, these tools may reduce repetitive programming effort and accelerate implementation. Nevertheless, security-sensitive code requires human review because AI-generated outputs can contain vulnerabilities or contextually inappropriate solutions (Black et al., 2024; Nguyen & Nadi, 2022; Perry et al., 2023). When AI assistance is combined with disciplined validation and secure development practices, it may contribute to faster and more consistent system development.

H1: AI-driven coding has a significant positive effect on secure payment gateway performance

2.3. Machine learning fraud detection

Machine learning fraud detection uses transaction histories, behavioral patterns, anomaly signals, and risk-scoring models to identify suspicious payment behavior. Fraud-detection problems are challenging because transaction streams can be high-volume, imbalanced, time-sensitive, and adaptive to changing attacker behavior (Abdallah et al., 2016; Jurgovsky et al., 2018). More recent hybrid approaches combine conventional machine-learning and deep-learning methods for real-time digital-payment fraud detection (Ingle et al., 2025). Effective fraud detection is therefore expected to improve the security and reliability dimensions of payment-gateway performance.

H2: Machine learning fraud detection has a significant positive effect on secure payment gateway performance.

2.4. Blockchain-enable security control

Blockchain-enabled security control refers to the use of distributed ledgers, tamper-resistant records, smart-contract logic, and decentralized verification to strengthen transaction integrity and traceability (Casino et al., 2019; Fachrian et al., 2024; Kshetri, 2017). The performance benefit is not automatic; suitability depends on architecture, governance, interoperability, and implementation cost. Sustainability research further shows that blockchain design choices can produce materially different energy and environmental footprints (Mulligan et al., 2024; Sai & Vranken, 2024).

H3: Blockchain-enabled security control has a significant positive effect on secure payment gateway performance

2.5. Data compliance quality

Data compliance quality reflects the accuracy, completeness, governance, and appropriate handling of payment data. Reliable data are necessary for authentication, fraud detection, reconciliation, reporting, and security decisions. Poor-quality or weakly governed data can reduce the usefulness of AI/ML analytics and undermine assurance processes (Cai & Zhu, 2015).

H4: Data compliance quality has a significant positive effect on secure payment gateway performance

2.6. API integration reliability

API integration reliability refers to stable, consistent, and fault-tolerant communication between the payment gateway and connected services such as banks, merchants, fraud engines, tokenization services, and blockchain networks. Microservice and API-based architectures depend on reliable service interaction, fault handling, and interoperability to reduce outages, latency, and transaction failures (Dragoni et al., 2017; Pautasso et al., 2017; Taibi et al., 2018).

H5: API integration reliability has a significant positive effect on secure payment gateway performance.

2.7. Payment gateway compliance

Payment gateway compliance captures adherence to security requirements, service-quality expectations, governance procedures, and operational controls. In digital finance, regulatory and operational compliance supports trust and reduces uncertainty in platform-based transactions (Gomber et al., 2017).

H6: Payment gateway compliance has a significant positive effect on secure payment gateway performance.

2.8. Security assurance quality and blockchain trust mechanism

Security assurance quality reflects the perceived strength of security controls, testing, monitoring, incident prevention, and protective practices. Blockchain trust mechanism reflects transparency, verifiability, resistance to unauthorized alteration, and confidence enabled by distributed-ledger characteristics (Casino et al., 2019; Kshetri, 2017). Both mechanisms may affect payment-gateway performance directly and may also shape the effectiveness of selected security-control relationships.

H7: Security assurance quality has a significant positive effect on secure payment gateway performance.

H8: Blockchain trust mechanism has a significant positive effect on secure payment gateway performance

2.9. Mediation and moderation hypotheses

Mediation evaluates whether the effect of a predictor on an outcome is transmitted through an intervening mechanism, while moderation evaluates whether the magnitude of a relationship changes across levels of another variable (Hayes & Rockwood, 2020).

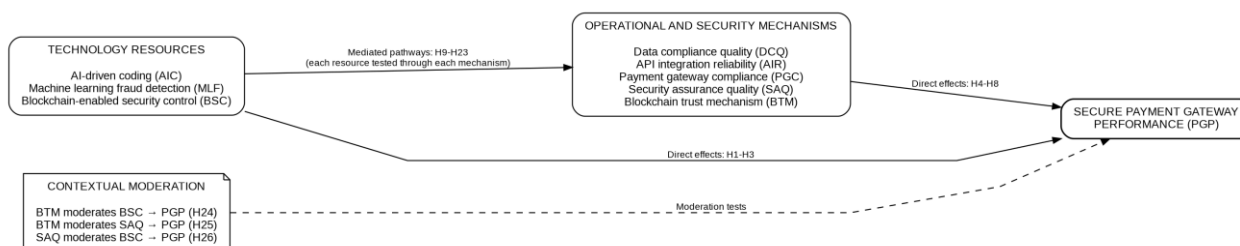


Figure 1. Conceptual framework. Solid pathways represent the tested direct and mediated relationships; dashed representation in the figure summarizes the three moderation tests

In this study, AIR, PGC, SAQ, BTM, and DCQ are examined as mechanisms through which AIC, MLF, and BSC may influence PGP. BTM and SAQ are also tested as moderators of selected relationships (Figure 1).

H9: AIR mediates the relationship between AIC and PGP.

H10: AIR mediates the relationship between MLF and PGP.

H11: AIR mediates the relationship between BSC and PGP.

H12: PGC mediates the relationship between AIC and PGP.

H13: PGC mediates the relationship between MLF and PGP.

H14: PGC mediates the relationship between BSC and PGP.

H15: SAQ mediates the relationship between AIC and PGP.

H16: SAQ mediates the relationship between MLF and PGP.

H17: SAQ mediates the relationship between BSC and PGP.

H18: BTM mediates the relationship between AIC and PGP.

H19: BTM mediates the relationship between MLF and PGP.

H20: BTM mediates the relationship between BSC and PGP.

H21: DCQ mediates the relationship between AIC and PGP.
H22: DCQ mediates the relationship between MLF and PGP.
H23: DCQ mediates the relationship between BSC and PGP.
H24: BTM moderates the relationship between BSC and PGP.
H25: BTM moderates the relationship between SAQ and PGP.
H26: SAQ moderates the relationship between BSC and PGP

3. MATERIAL AND METHODS

3.1 Research Design

A quantitative cross-sectional survey design was used to examine relationships among multiple reflective latent constructs. The analysis sequence comprised data screening, reliability assessment, sampling-adequacy checks, common-method and multicollinearity diagnostics, confirmatory factor analysis (CFA), covariance-based structural equation modeling (SEM), bootstrapped mediation analysis, and moderation with simple-slope analysis. Covariance-based SEM is appropriate when the objective is to evaluate a theory-specified measurement and structural model simultaneously (Dash & Paul, 2021; Shi et al., 2019).

3.2. Sample and Respondents

The final usable sample contained 500 respondents with relevant knowledge or experience in software development, data science, blockchain, API integration, payment-gateway systems, and other information-technology domains. The sample included software developers (31.4%), system analysts (15.4%), students (12.0%), data scientists or machine-learning engineers (10.8%), payment-system developers (10.0%), blockchain developers (9.4%), IT managers (8.4%), and other roles (2.6%). Most respondents reported prior experience with payment-gateway systems: 40.0% reported moderate experience, 25.2% advanced experience, and 8.8% expert-level experience. The sample size was sufficient for the reported CFA, SEM, mediation, and moderation analyses, although the generalizability of the findings remains dependent on the recruitment process and characteristics of the respondent pool (Sarstedt et al., 2020).

Participants were recruited in Myanmar in May 2026. The questionnaire was administered primarily through Google Forms distributed via social media, with additional responses collected through offline survey administration. Eligibility was restricted to individuals aged 18 years or older who had relevant knowledge or experience in artificial intelligence, machine learning, information technology, software development, API integration, blockchain technology, or payment systems. Individuals who did not meet these criteria were not eligible to participate

3.3. Measurement Instrument

Nine constructs were measured using seven items each on a five-point Likert scale ranging from 1 (strongly

disagree) to 5 (strongly agree): AIC, MLF, BSC, DCQ, AIR, PGC, SAQ, BTM, and PGP. Measurement quality was assessed using Cronbach's alpha, standardized factor loadings, composite reliability (CR), average variance extracted (AVE), the Fornell-Larcker criterion, and the heterotrait-monotrait ratio (HTMT) (Franke & Sarstedt, 2019; Henseler et al., 2015; Voorhees et al., 2016).

The questionnaire items were developed by the authors from the conceptual definitions of the constructs and the supporting literature cited in this study rather than reproduced verbatim from a single established scale. A pilot study involving 50 participants was conducted before the main data collection to assess clarity, comprehensibility, and practical administration of the instrument. Data analysis was performed using IBM SPSS Statistics version 23 and IBM SPSS AMOS version 24.

3.4. Data Analysis

Descriptive statistics were calculated for the constructs and respondent profile. Internal consistency was assessed with Cronbach's alpha. KMO and Bartlett's test were used to examine sampling adequacy and factorability. Harman's single-factor result was used as a basic diagnostic for a dominant common-method factor, while VIF, tolerance, and Mahalanobis distance were reported as additional diagnostics. Because Harman's test alone cannot rule out common-method bias, its result is interpreted as a screening indicator rather than definitive evidence (Kock et al., 2021). CFA assessed model fit and factor loadings; CR, AVE, Fornell-Larcker, and HTMT were used to evaluate convergent and discriminant validity (Franke & Sarstedt, 2019; Henseler et al., 2015; Voorhees et al., 2016). SEM then estimated direct effects, bootstrapped confidence intervals were used for indirect effects, and interaction terms were evaluated with false-discovery-rate (FDR) correction and simple slopes at low (-1 SD), mean, and high (+1 SD) moderator levels.

Formal ethics committee approval or waiver was not obtained for this study. Before completing the questionnaire, respondents were provided with information describing the purpose of the study, voluntary participation, confidentiality, absence of financial incentives, and their right to discontinue before submitting a response. Only respondents who indicated that they agreed to participate voluntarily were permitted to proceed with the survey. No ethics committee name or approval reference number is therefore available to report

4. RESULTS

4.1 Participant Characteristics

The final sample consisted of 500 respondents. Men represented 54.4% of the sample and women 43.2%; 1.6% preferred not to disclose gender and 0.8% selected another category. Respondents were predominantly between 20 and 30 years of age. Bachelor's degree

holders formed the largest education group (54.6%), followed by master's degree holders (29.4%). Software

developers were the largest occupational group (31.4%) (Table 1).

Table 1. Demographic profile of respondents

Variable	Category	Frequency	Percentage
Gender	Male	272	54.40%
	Female	216	43.20%
	Prefer not to say	8	1.60%
	Other	4	0.80%
Age	Below 20 years old	24	4.80%
	20–25 years old	156	31.20%
	26–30 years old	150	30.00%
	31–35 years old	84	16.80%
	36–40 years old	54	10.80%
	Above 40 years old	32	6.40%
Highest Education Level	Diploma	41	8.20%
	Bachelor's Degree	273	54.60%
	Master's Degree	147	29.40%
	PhD	24	4.80%
	Other	15	3.00%
Current Role	Software Developer	157	31.40%
	System Analyst	77	15.40%
	Student	60	12.00%
	Data Scientist / Machine Learning Engineer	54	10.80%
	Payment System Developer	50	10.00%
	Blockchain Developer	47	9.40%
	IT Manager	42	8.40%
	Other	13	2.60%
Experience with Payment Gateway Systems	No experience	29	5.80%
	Basic experience	101	20.20%
	Moderate experience	200	40.00%
	Advanced experience	126	25.20%
	Expert level	44	8.80%
Main Programming Language Used	Python	124	24.80%
	JavaScript	121	24.20%
Main Programming Language Used Main Programming Language Used	Java	85	17.00%
	PHP	67	13.40%
	C#	54	10.80%
	Solidity	31	6.20%
	Other	18	3.60%

Source: Survey Data 2026

4.2 Descriptive Statistics

3.51 to 3.58, indicating moderate agreement overall, and standard deviations ranged from 0.69 to 0.74 (Table 2).

All nine constructs had 500 valid observations with no missing construct-level data. Mean values ranged from

Table 2. Composite construct descriptive statistics

Construct	Items	N	Missing	Mean	SD	Minimum	Maximum
AIC	7	500	0	3.55	0.69	1.571	5
MLF	7	500	0	3.52	0.71	1.143	5
BSC	7	500	0	3.51	0.74	1.143	5
DCQ	7	500	0	3.54	0.73	1.571	5
AIR	7	500	0	3.55	0.74	1	5
PGC	7	500	0	3.58	0.72	1.571	5
SAQ	7	500	0	3.54	0.73	1.429	5
BTM	7	500	0	3.52	0.73	1.286	5
PGP	7	500	0	3.53	0.69	1.714	5

Source: Survey Data 2026

4.3. Reliability, Sampling Adequacy, Common-Method Diagnostics, and Multicollinearity

Cronbach's alpha values ranged from 0.884 to 0.903, indicating high internal consistency. KMO was 0.956 and Bartlett's test was significant ($\chi^2 = 17,568.381$, $df = 1,953$, $p < .001$). The first Harman factor accounted for 29.25% of variance, which does not indicate a dominant single-factor pattern; however, this test alone cannot exclude common-method bias. The highest VIF was 2.16 and the lowest tolerance was 0.463, indicating no severe multicollinearity in the reported diagnostics (Table 3)

Table 3. Reliability, KMO, common-method, VIF, and outlier summary

Metric / Construct	Result	Decision
AIC Cronbach Alpha	0.884	Accepted
MLF Cronbach Alpha	0.884	Accepted
BSC Cronbach Alpha	0.898	Accepted
DCQ Cronbach Alpha	0.897	Accepted
AIR Cronbach Alpha	0.903	Accepted
PGC Cronbach Alpha	0.893	Accepted
SAQ Cronbach Alpha	0.896	Accepted
BTM Cronbach Alpha	0.895	Accepted
PGP Cronbach Alpha	0.885	Accepted
KMO	0.956	Excellent
Bartlett Approx. Chi-square	17568.381	Accepted
Bartlett df	1953	Accepted
Bartlett Sig.	$p < .001$	Accepted
Harman first factor	29.25%	Accepted
Highest VIF	2.16	Accepted
Lowest tolerance	0.463	Accepted
Mahalanobis maximum	21.642	Accepted

Source: Survey Data 2026

4.4. Correlation analysis

An aircraft hangar is a closed structure which is constructed for the use of servicing and maintenance of various aircraft as a protective space because whenever an aircraft arrival be seen after a long journey it has to be taken under that hangar where all the equipment's are available for it servicing. In an aircraft hangar more space is required for its storage and extra space for its maintenance.

Table 4. Construct correlation matrix Pannel A

Construct	AIC	MLF	BSC	DCQ	AIR
AIC	1	0.191	0.221	0.397	0.425
MLF	0.191	1	0.251	0.255	0.334
BSC	0.221	0.251	1	0.261	0.345
DCQ	0.397	0.255	0.261	1	0.536
AIR	0.425	0.334	0.345	0.536	1
PGC	0.277	0.449	0.356	0.368	0.528
SAQ	0.411	0.479	0.438	0.494	0.572
BTM	0.205	0.3	0.472	0.321	0.402
PGP	0.446	0.446	0.427	0.449	0.561

Source: Survey Data 2026

Majority of the hangars are design as a pre-engineered steel building due to its light weight and higher resistance over wind and seismic loads.

Table 5. Construct correlation matrix Pannel B

Construct	PGC	SAQ	BTM	PGP
AIC	0.277	0.411	0.205	0.446
MLF	0.449	0.479	0.3	0.446
BSC	0.356	0.438	0.472	0.427
DCQ	0.368	0.494	0.321	0.449
AIR	0.528	0.572	0.402	0.561
PGC	1	0.557	0.399	0.533
SAQ	0.557	1	0.35	0.646
BTM	0.399	0.35	1	0.453
PGP	0.533	0.646	0.453	1

Source: Survey Data 2026

Construct correlation matrix for Pannel A and Panel B are presented in Table 4 and Table 5.

4.5. CFA Measurement Model

The CFA results indicated acceptable overall model fit. CMIN/DF was 1.063, RMR was 0.026, IFI/TLI/CFI were 0.993, and RMSEA was 0.011 with PCLOSE = 1.000. GFI (0.894), NFI (0.893), and RFI (0.887) were slightly below the conventional 0.90 preference, so the fit is better characterized as acceptable to strong overall rather than uniformly excellent. Standardized loadings ranged from 0.682 to 0.778

Figure 2. CFA measurement model summary. Values show standardized loading ranges, composite reliability (CR), average variance extracted (AVE), and overall model-fit indices (table 6). CFA Factor Loading Summary is presented in Table 7.

Table 6. CFA model fit indices

Index	Value	Recommended Rule
CMIN	1969.94	Report value
DF	1854	Report value
p	0.03	Can be significant with large N
CMIN/DF	1.063	< 3 preferred; < 5 acceptable
RMR	0.026	< 0.05 good
GFI	0.894	≥ 0.90 preferred
AGFI	0.884	≥ 0.80 acceptable
PGFI	0.822	Higher is better
NFI	0.893	≥ 0.90 preferred
RFI	0.887	≥ 0.90 preferred
IFI	0.993	≥ 0.90
TLI	0.993	≥ 0.90
CFI	0.993	≥ 0.90
RMSEA	0.011	< 0.08 acceptable; < 0.05 excellent
PCLOSE	1	> 0.05

Source: Survey Data 2026

Retained indicators: seven items per construct; standardized loading ranges shown below

AIC: AI-driven coding Loading = .690–.760 CR = .885 AVE = .524	MLF: ML fraud detection Loading = .686–.758 CR = .884 AVE = .522	BSC: Blockchain security control Loading = .708–.770 CR = .898 AVE = .558
DCQ: Data compliance quality Loading = .730–.769 CR = .898 AVE = .556	AIR: API integration reliability Loading = .735–.771 CR = .903 AVE = .571	PGC: Payment gateway compliance Loading = .719–.758 CR = .893 AVE = .544
SAQ: Security assurance quality Loading = .710–.778 CR = .896 AVE = .553	BTM: Blockchain trust mechanism Loading = .716–.764 CR = .895 AVE = .550	PGP: Payment gateway performance Loading = .682–.756 CR = .885 AVE = .525

Model fit: CMIN/DF = 1.063 | CFI = .993 | TLI = .993 | RMSEA = .011

Figure 2. CFA Measurement model summary

Source: Survey Data 2026

Table 7. CFA Factor Loading Summary

Construct	Standardized Loading Range	Decision
AIC	0.690–0.760	Accepted
MLF	0.686–0.758	Accepted
BSC	0.708–0.770	Accepted
DCQ	0.730–0.769	Accepted
AIR	0.735–0.771	Accepted
PGC	0.719–0.758	Accepted
SAQ	0.710–0.778	Accepted
BTM	0.716–0.764	Accepted
PGP	0.682–0.756	Accepted

Source: Survey Data 2026

4.6. Convergent and Discriminant Validity

Composite reliability values ranged from 0.884 to 0.903 and all AVE values exceeded 0.50, supporting internal consistency and convergent validity. In the Fornell-Larcker matrix, each square root of AVE exceeded the corresponding inter-construct correlations. HTMT values were below conventional thresholds, with the highest reported value equal to 0.725 between SAQ and PGP.

Table 8. Composite reliability and average variance extracted Panel A

Construct	CR	AVE	$\sqrt{\text{AVE}}$	Min Loading
AIC	0.885	0.524	0.724	0.69
MLF	0.884	0.522	0.723	0.686
BSC	0.898	0.558	0.747	0.708
DCQ	0.898	0.556	0.746	0.73
AIR	0.903	0.571	0.756	0.735
PGC	0.893	0.544	0.738	0.719
SAQ	0.896	0.553	0.744	0.71
BTM	0.895	0.55	0.742	0.716
PGP	0.885	0.525	0.725	0.682

Source: Survey Data 2026

Table 9. Composite reliability and average variance extracted Panel B

Construct	Max Loading	CR Decision	AVE Decision
AIC	0.76	Accept	Accept
MLF	0.758	Accept	Accept
BSC	0.77	Accept	Accept
DCQ	0.769	Accept	Accept
AIR	0.771	Accept	Accept
PGC	0.758	Accept	Accept
SAQ	0.778	Accept	Accept
BTM	0.764	Accept	Accept
PGP	0.756	Accept	Accept

Source: Survey Data 2026

Table 10. Fornell-Larcker criterion Panel A

Construct	AIC	MLF	BSC	DCQ	AIR
AIC	0.72	0.19	0.22	0.397	0.43
MLF	0.19	0.72	0.25	0.255	0.33
BSC	0.22	0.25	0.75	0.261	0.35
DCQ	0.4	0.26	0.26	0.746	0.54
AIR	0.43	0.33	0.35	0.536	0.76
PGC	0.28	0.45	0.36	0.368	0.53
SAQ	0.41	0.48	0.44	0.494	0.57
BTM	0.21	0.3	0.47	0.321	0.4
PGP	0.45	0.45	0.43	0.449	0.56

Source: Survey Data 2026

Table 11. Fornell-Larcker criterion Panel B

Construct	PGC	SAQ	BTM	PGP
AIC	0.28	0.41	0.21	0.446
MLF	0.45	0.48	0.3	0.446
BSC	0.36	0.44	0.47	0.427
DCQ	0.37	0.49	0.32	0.449
AIR	0.53	0.57	0.4	0.561
PGC	0.74	0.56	0.4	0.533
SAQ	0.56	0.74	0.35	0.646
BTM	0.4	0.35	0.74	0.453
PGP	0.53	0.65	0.45	0.725

Source: Survey Data 2026

Table 12. HTMT Ratio Matrix Panel A

Construct	AIC	MLF	BSC	DCQ	AIR
AIC	1	0.22	0.25	0.446	0.48
MLF	0.22	1	0.28	0.286	0.37
BSC	0.25	0.28	1	0.29	0.38
DCQ	0.45	0.29	0.29	1	0.6
AIR	0.48	0.37	0.38	0.595	1
PGC	0.31	0.51	0.4	0.411	0.59
SAQ	0.46	0.54	0.49	0.551	0.64
BTM	0.23	0.34	0.53	0.357	0.45
PGP	0.5	0.5	0.48	0.504	0.63

Source: Survey Data 2026

Table 13. HTMT Ratio Matrix Panel B

Construct	PGC	SAQ	BTM	PGP
AIC	0.31	0.46	0.23	0.504
MLF	0.51	0.54	0.34	0.504
BSC	0.4	0.49	0.53	0.479
DCQ	0.41	0.55	0.36	0.504
AIR	0.59	0.64	0.45	0.627
PGC	1	0.62	0.45	0.6
SAQ	0.62	1	0.39	0.725
BTM	0.45	0.39	1	0.508
PGP	0.6	0.73	0.51	1

Source: Survey Data 2026

Composite reliability and average variance extracted for Panel A Table 8, for B Table 9, Fornell-Larcker criterion for Panel A Table 10, for B Table 11, HTMT Ratio Matrix Panel A Table 12 and B Table 13.

4.7. SEM Structural Model and Direct Effects

Five of the eight direct hypotheses were supported. AIC ($\beta = 0.176$, $p < .001$), MLF ($\beta = 0.114$, $p = .010$), AIR ($\beta = 0.123$, $p = .027$), SAQ ($\beta = 0.337$, $p < .001$), and BTM ($\beta = 0.164$, $p < .001$) had significant positive direct effects on PGP. BSC, DCQ, and PGC did not show statistically significant direct effects at the 0.05 level. SAQ had the largest standardized direct effect. The structural model explained 64.6% of the variance in secure payment gateway performance ($R^2 = 0.646$), indicating substantial explanatory capacity.

Table 14. Direct SEM Hypothesis Testing Panel A

Hypothesis	Path	Estimate	S.E.
H1	AIC → PGP	0.181	0.04
H2	MLF → PGP	0.112	0.04
H3	BSC → PGP	0.055	0.04
H4	DCQ → PGP	0.014	0.05
H5	AIR → PGP	0.112	0.05
H6	PGC → PGP	0.096	0.05
H7	SAQ → PGP	0.345	0.07
H8	BTM → PGP	0.158	0.05

Source: Survey Data 2026

Figure 3. Final SEM structural model summary for secure payment gateway performance. The upper panel reports direct effects with standardized path coefficients (β), p-values, and explained variance (R^2); dashed arrows indicate non-significant direct paths.

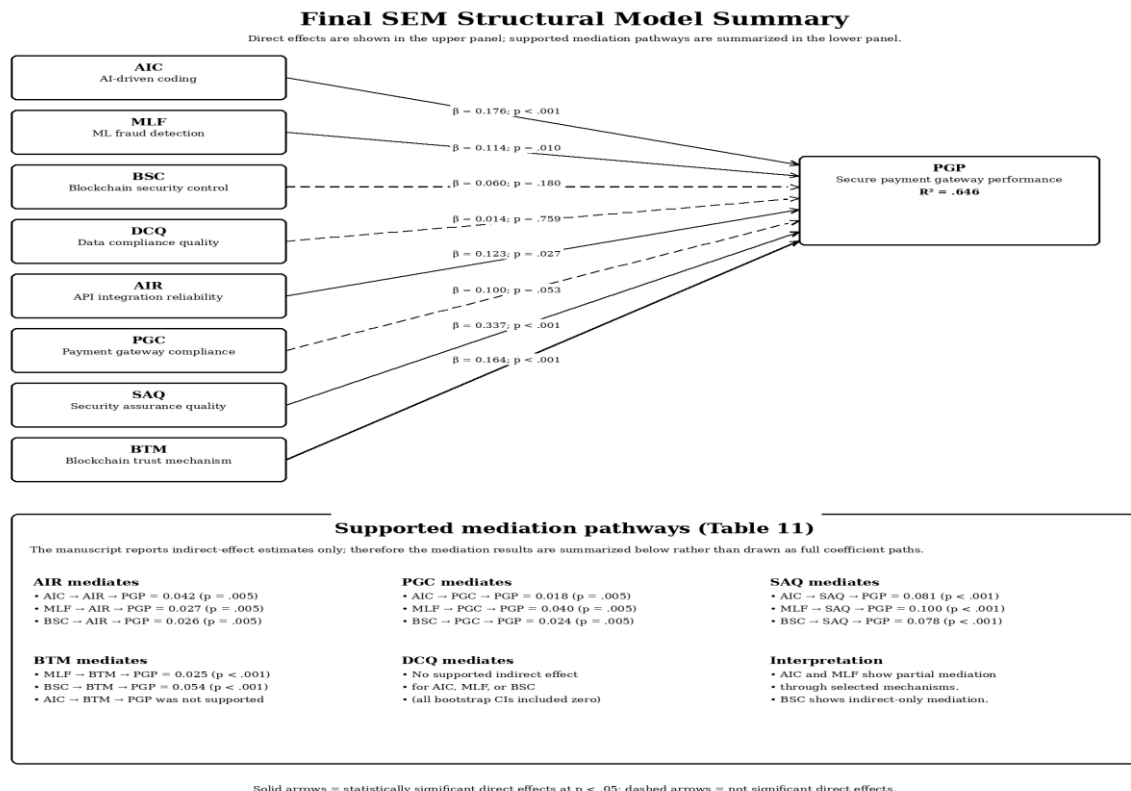


Figure 3. Final SEM structural model (Source: Survey Data 2026)

Table 15. Direct SEM Hypothesis Testing Panel B

Hypothesis	C.R.	β	p-value	Decision
H1	4.115	0.176	< .001	Supported
H2	2.564	0.114	0.01	Supported
H3	1.341	0.06	0.18	Not supported
H4	0.307	0.014	0.76	Not supported
H5	2.209	0.123	0.03	Supported
H6	1.938	0.1	0.05	Not supported
H7	5.208	0.337	< .001	Supported
H8	3.536	0.164	< .001	Supported

Source: Survey Data 2026

Direct SEM Hypothesis Testing Panel A is presented in Table 4 and for Panel B Table 15.

4.8. Mediation Analysis

Eleven of the 15 tested indirect effects were supported. AIR, PGC, and SAQ significantly mediated the relationships of AIC, MLF, and BSC with PGP. BTM mediated the MLF→PGP and BSC→PGP relationships but not AIC→PGP, while DCQ did not significantly mediate any of the three technology-resource relationships. Because the direct BSC→PGP path was not significant, the supported BSC indirect paths are more accurately described as indirect-only mediation rather than partial mediation. The supported AIC and MLF indirect paths coexist with significant direct effects and are therefore consistent with partial mediation

Table 16. Mediation analysis with bootstrap confidence intervals Panel A

IV	Mediator	DV	Indirect Effect	Boot LL
AIC	DCQ	PGP	0.014	-0.013
MLF	DCQ	PGP	0.006	-0.006
BSC	DCQ	PGP	0.006	-0.006
AIC	AIR	PGP	0.042	0.013
MLF	AIR	PGP	0.027	0.007
BSC	AIR	PGP	0.026	0.008
AIC	PGC	PGP	0.018	0.005
MLF	PGC	PGP	0.04	0.013
BSC	PGC	PGP	0.024	0.007
AIC	SAQ	PGP	0.081	0.05
MLF	SAQ	PGP	0.1	0.064
BSC	SAQ	PGP	0.078	0.048
AIC	BTM	PGP	0.011	-0.001
MLF	BTM	PGP	0.025	0.01
BSC	BTM	PGP	0.054	0.025

Source: Survey Data 2026

Table 17. Mediation analysis with bootstrap confidence intervals Panel B

IV	Boot UL	Boot p	Decision	Mediation Type
AIC	0.041	0.319	Not supported	No mediation
MLF	0.02	0.32	Not supported	No mediation
BSC	0.019	0.32	Not supported	No mediation
AIC	0.073	0.005	Supported	Partial mediation

MLF	0.05	0.005	Supported	Partial mediation
BSC	0.046	0.005	Supported	Indirect-only mediation
AIC	0.035	0.005	Supported	Partial mediation
MLF	0.072	0.005	Supported	Partial mediation
BSC	0.046	0.005	Supported	Indirect-only mediation
AIC	0.114	< .001	Supported	Partial mediation
MLF	0.137	< .001	Supported	Partial mediation
BSC	0.11	< .001	Supported	Indirect-only mediation
AIC	0.026	0.068	Not supported	No mediation
MLF	0.044	< .001	Supported	Partial mediation
BSC	0.084	< .001	Supported	Indirect-only mediation

Source: Survey Data 2026

Mediation analysis with bootstrap confidence intervals Panel A is presented in Table 16 and for panel B table 17.

4.9. Moderation and Simple-slope Analysis

All three tested interaction effects were supported after FDR correction. BTM moderated the BSC→PGP relationship ($B = 0.149$, $FDR\ p = .001$) and the SAQ→PGP relationship ($B = 0.148$, $FDR\ p = .001$), while SAQ moderated the BSC→PGP relationship ($B = 0.105$, $FDR\ p = .039$). Simple-slope results indicate that the BSC effect becomes positive and significant at mean and high levels of BTM and SAQ, whereas the corresponding low-moderator slopes are not significant. The SAQ→PGP relationship remains significant across low, mean, and high BTM levels and becomes stronger as BTM increases

Table 18. Moderation effects (interaction = $X \times$ moderator) Panel A

X	Moderator	B	SE	t	p
BSC	BTM	0.15	0	4.1	< .001
SAQ	BTM	0.15	0	4	< .001
BSC	SAQ	0.11	0	2.9	0.004

Source: Survey Data 2026

Table 19. Moderation effects (interaction = $X \times$ moderator) Panel B

X	FDR p	Bootstrap 95% CI	ΔR^2	Decision
BSC	0.001	[0.08, 0.21]	0	Supported
SAQ	0.001	[0.08, 0.21]	0	Supported
BSC	0.039	[0.03, 0.17]	0	Supported

Source: Survey Data 2026

Table 20. Simple-slope Analysis Panel A

X	Moderator	Moderator Level	Slope B	SE
BSC	BTM	Low (-1 SD)	-0.03	0.04
BSC	BTM	Mean	0.08	0.03
BSC	BTM	High (+1 SD)	0.19	0.04

SAQ	BTM	Low (-1 SD)	0.167	0.05
SAQ	BTM	Mean	0.275	0.04
SAQ	BTM	High (+1 SD)	0.384	0.05
BSC	SAQ	Low (-1 SD)	0	0.04
BSC	SAQ	Mean	0.077	0.03
BSC	SAQ	High (+1 SD)	0.154	0.04

Source: Survey Data 2026

Table 21. Simple-slope Analysis Pannel B

X	t	p	95% CI	Decision
BSC	-0.7	0.482	[-0.11, 0.05]	Not significant
BSC	2.396	0.017	[0.014, 0.15]	Significant
BSC	4.316	< .001	[0.103, 0.28]	Significant
SAQ	3.399	0.001	[0.07, 0.26]	Significant
SAQ	6.663	< .001	[0.194, 0.36]	Significant
SAQ	7.669	< .001	[0.285, 0.48]	Significant
BSC	0	0.998	[-0.08, 0.08]	Not significant
BSC	2.272	0.024	[0.01, 0.14]	Significant
BSC	3.484	0.001	[0.067, 0.24]	Significant

Source: Survey Data 2026

Moderation effects (interaction = $X \times \text{moderator}$) Pannel A is presented in Table 18, for panel B Table 19. Simple-slope Analysis Pannel A is presented in Table 20, and for panel B table 21,

5. DISCUSSION

The results show that secure payment gateway performance is associated with a combination of development, fraud-detection, integration, assurance, and trust capabilities rather than with a single technology. SAQ produced the strongest direct effect, emphasizing that security controls, monitoring, testing, and incident-prevention quality are central to perceived gateway performance. This result is consistent with broader digital-payment research showing that cybersecurity is closely tied to trust and continued use (Aljaradat et al., 2024).

AIC and MLF also had significant direct effects. The AIC finding should not be interpreted as evidence that AI-generated code is inherently secure. Prior studies show that AI coding assistants can produce insecure code and that security depends on validation, prompting practices, model behavior, and human review (Black et al., 2024; Perry et al., 2023). The result instead suggests that, within the surveyed population, AI-assisted development capability is positively associated with PGP when considered alongside other system and security mechanisms. The MLF result is consistent with the long-standing role of anomaly detection and classification in financial fraud prevention (Abdallah et al., 2016; Ingle et al., 2025; Jurgovsky et al., 2018).

BSC did not have a significant direct effect on PGP, but several BSC indirect effects were significant. This pattern suggests that blockchain-enabled control may contribute to performance when it is translated into concrete operational mechanisms such as reliable APIs, gateway compliance, security assurance, or blockchain-enabled trust. Recent work on blockchain-based payment-record integrity similarly emphasizes implementation architecture rather than blockchain adoption alone (Fachrian et al., 2024).

The mediation results clarify the mechanism of influence. SAQ generated the largest reported indirect effect for $MLF \rightarrow SAQ \rightarrow PGP$ (0.100), and AIR and PGC also carried significant indirect effects. For BSC, the significant indirect paths combined with a non-significant direct path indicate indirect-only mediation. This distinction is theoretically useful because it shifts attention from technology possession to the capabilities through which technology is operationalized.

5.1 Sustainable Computing and Cybersecurity Implications

From a sustainable-computing perspective, the relevance of this study is strongest in sustainable cybersecurity and resilient digital infrastructure. Sustainable cybersecurity research emphasizes that security should support long-term system resilience while recognizing resource and environmental trade-offs (Achuthan et al., 2025; Morales-Sáenz et al., 2024). The present findings suggest that assurance quality, reliable integration, fraud detection, and trust mechanisms are important operational capabilities for maintaining dependable payment services. Such reliability can support the continuity and sustainability of digital commerce by reducing failure, fraud exposure, and trust erosion.

However, the empirical model does not measure energy consumption, computation cost, carbon emissions, hardware utilization, or blockchain consensus efficiency. Therefore, it would be inappropriate to claim that the tested model demonstrates environmental sustainability. Recent blockchain-sustainability research explicitly warns that environmental performance depends on platform architecture and measurement assumptions (Mulligan et al., 2024; Sai & Vranken, 2024). Future extensions should combine the present security-performance model with energy-per-transaction, latency, computational overhead, carbon intensity, and lifecycle resource indicators so that security, performance, and environmental sustainability can be evaluated together

5.2. Partial Implications

For payment-gateway providers and software teams, the findings support a layered implementation strategy. AI-assisted coding should be paired with secure review and testing rather than treated as autonomous code production. Fraud-detection capability should be integrated with dependable APIs and transaction monitoring. Security assurance deserves particular

attention because it showed the strongest direct effect and also carried several indirect effects. Blockchain controls should be adopted selectively where traceability, tamper resistance, or inter-organizational trust justify the integration cost, and their design should consider both operational and environmental overhead.

5.3. Limitation and future research

Several limitations should be considered. First, the cross-sectional survey design identifies associations and does not establish causal effects. Second, the model relies on self-reported perceptions from a single survey instrument; although the reported Harman result did not indicate a dominant single factor, more rigorous procedural and statistical controls for common-method bias would strengthen future studies (Kock et al., 2021). Third, although respondents were recruited in Myanmar from several technology-related backgrounds, the recruitment approach and heterogeneous professional composition of the sample may limit population representativeness and the generalizability of the findings to other national, organizational, or payment-system contexts. Fourth, PGP is perception-based rather than derived from objective operational records such as latency, uptime, transaction failure rate, fraud-loss reduction, defect density, or incident frequency. Fifth, the model contains many constructs and indirect pathways, so independent replication and cross-validation in banking, fintech, and e-commerce settings are needed. Finally, environmental sustainability was not measured. Future studies should incorporate resource-use and energy metrics and compare blockchain and non-blockchain architectures under equivalent security and performance requirements.

6. CONCLUSIONS

This study develops and tests an integrated model of secure payment gateway performance using data from 500 technical respondents. AIC, MLF, AIR, SAQ, and BTM had significant positive direct effects on PGP, with SAQ showing the strongest standardized direct effect. Eleven indirect effects were supported, and the BSC pathways were primarily expressed through indirect

operational mechanisms rather than a significant direct effect. Three moderation effects involving BTM and SAQ were also supported after FDR correction. Overall, the results indicate that payment-gateway performance is shaped by the interaction between technology resources and the operational capabilities that translate those resources into reliable, secure, and trusted services. For sustainable-computing research, the contribution is currently limited to the resilience and sustainability-cybersecurity dimensions; environmental sustainability should be tested directly in future work using measurable energy and resource indicators:

Funding

The authors received no external financial support for the research, authorship, or publication of this article.

Conflicts of Interest

The authors declare that they have no financial or non-financial conflicts of interest that could be perceived as influencing the submitted work.

Data Availability

The anonymized survey data supporting the findings of this study are available from the corresponding author upon reasonable request, subject to confidentiality and applicable data-sharing restrictions. The questionnaire and informed-consent materials are also available from the corresponding author upon reasonable request

Author Contributions

Thaingar Aung Soe contributed to the conception and design of the study, questionnaire development, data collection, statistical analysis, interpretation of the results, and drafting of the manuscript.

Arkar Htet contributed to the research design, literature review, interpretation of the findings, methodological review, and critical revision of the manuscript for important intellectual content.

Yu Thwe contributed to the literature review, questionnaire review, data interpretation, manuscript preparation, proofreading, and critical review of the final manuscript.

All authors reviewed and approved the final version of the manuscript and agreed to be accountable for the accuracy and integrity of the work.

References

- Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, 68, 90–113. DOI:10.1016/j.jnca.2016.04.007
- Achuthan, K., Sankaran, S., Roy, S., & Raman, R. (2025). Integrating sustainability into cybersecurity: Insights from machine learning based topic modeling. *Discover Sustainability*, 6, 44. DOI:10.1007/s43621-024-00754-w
- Aljaradat, A., Sarkar, G., & Shukla, S. K. (2024). Modelling cybersecurity impacts on digital payment adoption: A game theoretic approach. *Journal of Economic Criminology*, 5, 100089. DOI:10.1016/j.jeconc.2024.100089
- Allamanis, M., Barr, E. T., Devanbu, P., & Sutton, C. (2018). A survey of machine learning for big code and naturalness. *ACM Computing Surveys*, 51, 81. DOI:10.1145/3212695

- Black, G. S., Rimal, B. P., & Vaidyan, V. M. (2024). Balancing security and correctness in code generation: An empirical study on commercial large language models. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 1–12. DOI:10.1109/TETCI.2024.3446695
- Cai, L., & Zhu, Y. (2015). The challenges of data quality and data quality assessment in the big data era. *Data Science Journal*, 14, 2. DOI:10.5334/dsj-2015-002
- Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81. DOI:10.1016/j.tele.2018.11.006
- Dash, G., & Paul, J. (2021). CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. *Technological Forecasting and Social Change*, 173, 121092. DOI:10.1016/j.techfore.2021.121092
- Dragoni, N., Giallorenzo, S., Lluch Lafuente, A., Mazzara, M., Montesi, F., Mustafin, R., & Safina, L. (2017). Microservices: Yesterday, today, and tomorrow. In M. Mazzara & B. Meyer (Eds.), *Present and ulterior software engineering* (pp. 195–216). Springer. DOI:10.1007/978-3-319-67425-4_12
- Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J. S., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., ... Williams, M. D. (2021). Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 57, 101994. DOI:10.1016/j.ijinfomgt.2019.08.002
- Fachrian, M. A., Sukarno, P., & Wardana, A. A. (2024). Decentralize transaction records of digital payment gateway using Ethereum Blockchain and Interplanetary File System. *Procedia Computer Science*, 237, 269–276. DOI:10.1016/j.procs.2024.05.105
- Franke, G., & Sarstedt, M. (2019). Heuristics versus statistics in discriminant validity testing: A comparison of four procedures. *Internet Research*, 29, 430–447. DOI:10.1108/INTR-12-2017-0515
- Gomber, P., Koch, J. A., & Siering, M. (2017). Digital finance and FinTech: Current research and future research directions. *Journal of Business Economics*, 87, 537–580. DOI:10.1007/s11573-017-0852-x
- Hayes, A. F., & Rockwood, N. J. (2020). Conditional process analysis: Concepts, computation, and advances in the modeling of the contingencies of mechanisms. *American Behavioral Scientist*, 64, 19–54. DOI:10.1177/0002764219859633
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43, 115–135. DOI:10.1007/s11747-014-0403-8
- Ingle, P., Mujumale, S. B., Pandhare, P. R., & Wasatkar, N. (2025). Artificial intelligence-driven fraud detection in digital payment systems: A hybrid machine learning approach. *2025 IEEE Pune Section International Conference (PuneCon)*. DOI:10.1109/PuneCon67554.2025.11378213
- Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications*, 100, 234–245. DOI:10.1016/j.eswa.2018.01.037
- Kock, F., Berbekova, A., & Assaf, A. G. (2021). Understanding and managing the threat of common method bias: Detection, prevention and control. *Tourism Management*, 86, 104330. DOI:10.1016/j.tourman.2021.104330
- Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 41, 1027–1038. DOI:10.1016/j.telpol.2017.09.003
- Li, Y., Choi, D., Chung, J., Kushman, N., Schrittwieser, J., Leblond, R., Eccles, T., Keeling, J., Gimeno, F., Dal Lago, A., Hubert, T., Choy, P., de Masson d'Autume, C., Babuschkin, I., Chen, X., Huang, P.-S., Welbl, J., Goyal, S., Cherepanov, A., ... Vinyals, O. (2022). Competition-level code generation with AlphaCode. *Science*, 378(6624), 1092–1097. DOI:10.1126/science.abq1158
- Morales-Sáenz, F. I., Medina-Quintero, J. M., & Reyna-Castillo, M. (2024). Beyond data protection: Exploring the convergence between cybersecurity and sustainable development in business. *Sustainability*, 16, 5884. DOI:10.3390/su16145884
- Mulligan, C., Morsfield, S., & Cheikosman, E. (2024). Blockchain for sustainability: A systematic literature review for policy impact. *Telecommunications Policy*, 48, 102676. DOI:10.1016/j.telpol.2023.102676
- Nguyen, N., & Nadi, S. (2022). An empirical evaluation of GitHub Copilot's code suggestions. *Proceedings of the 19th International Conference on Mining Software Repositories*, 1–5. DOI:10.1145/3524842.3528470
- Pautasso, C., Zimmermann, O., Amundsen, M., Lewis, J., & Josuttis, N. M. (2017). Microservices in practice, Part 1: Reality check and service design. *IEEE Software*, 34, 91–98. DOI:10.1109/MS.2017.24
- Perry, N., Srivastava, M., Kumar, D., & Boneh, D. (2023). Do users write more insecure code with AI assistants? *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2785–2799. DOI:10.1145/3576915.3623157
- Sai, A. R., & Vranken, H. (2024). Promoting rigor in blockchain energy and environmental footprint research: A systematic literature review. *Blockchain: Research and Applications*, 5, 100169. DOI:10.1016/j.bcra.2023.100169

- Sarstedt, M., Ringle, C. M., Cheah, J. H., Ting, H., Moisesescu, O. I., & Radomir, L. (2020). Structural model robustness checks in PLS-SEM. *Tourism Economics*, 26, 531–554. DOI:10.1177/1354816618823921
- Shi, D., Lee, T., & Maydeu-Olivares, A. (2019). Understanding the model size effect on SEM fit indices. *Educational and Psychological Measurement*, 79, 310–334. DOI:10.1177/0013164418783530
- Taibi, D., Lenarduzzi, V., & Pahl, C. (2018). Architectural patterns for microservices: A systematic mapping study. *Proceedings of the 8th International Conference on Cloud Computing and Services Science*, 221–232. DOI:10.5220/0006798302210232
- Vaithilingam, P., Zhang, T., & Glassman, E. L. (2022). Expectation vs. experience: Evaluating the usability of code generation tools powered by large language models. *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, 1–7. DOI:10.1145/3491101.3519665
- Voorhees, C. M., Brady, M. K., Calantone, R., & Ramirez, E. (2016). Discriminant validity testing in marketing: An analysis, causes for concern, and proposed remedies. *Journal of the Academy of Marketing Science*, 44, 119–134. DOI:10.1007/s11747-015-0455-4

Thaingar Aung Soe

Division of Computer Science
Country. United States of America
thaingaras@gmail.com
ORCID: 0009-0002-8278-7507

Arkar Htet

Research Scholar, Azteca
University, Division of
International, Mexico
arkarhm@gmail.com
ORCID: 0000-0003-1301-3604

Yu Thwe

Master of Business Administration,
Lincoln University College, Malaysia
yuthwe@gmail.com
ORCID: 0009-0004-9202-5017
