ACADEMIA: Jurnal Inovasi Riset Akademik
Vol. 6, No. 4, September-November 2026
e-ISSN : 2807-1808 | p-ISSN : 2807-2294
Online Journal System https://jurnalp4i.com/index.php/academia

DIGITAL TRANSFORMATION MARKETING STRATEGY FOR SECURITY SERVICES: A NICE MARKETING MIX APPROACH FOR AI AND IOT ADOPTION IN EMERGING MARKETS

Heru Hariyanto [1] , Rhian Indradewa [2] , Unggul Kustiawan [3] , Ketut Sunaryanto [4]
[1234] Universitas Esa Unggul, Indonesia
Email: heru.hariyanto@student.esaunggul.ac.id, rhian.indradewa@esaunggul.ac.id, unggul.kustiawan@esaunggul.ac.id, ketut.sunaryanto@esaunggul.ac.id

Diterima:20*/8/2026*; Direvisi: *31/8/2026*; Diterbitkan: *7/9/2026*

ABSTRAK

Transformasi digital telah menjadi agenda strategis yang krusial di seluruh layanan keamanan industri untuk mengatasi inefisiensi operasional dan keterbatasan visibilitas yang berulang. Namun, solusi keamanan berbasis teknologi menghadapi hambatan penerimaan pelanggan yang persisten di pasar berkembang *business-to-business* (B2B). Studi kuantitatif ini bertujuan merumuskan kerangka strategi pemasaran terintegrasi untuk layanan keamanan digital serta mengidentifikasi inisiatif prioritas yang mendukung adopsi teknologi. Data dikumpulkan melalui kuesioner terstruktur yang dibagikan kepada 19 pengambil keputusan keamanan perusahaan di berbagai sektor industri di wilayah Jabodetabek (*Greater Jakarta*). Penilaian kuantitatif menggunakan model evaluasi strategis multikriteria, termasuk matriks faktor internal-eksternal (*internal-external factor matrices*) dan matriks prioritas strategis (*strategic priority matrices*). Temuan empiris mengungkapkan bahwa kesulitan pengukuran kinerja berbasis data dan keterlambatan pelaporan merupakan titik masalah pelanggan (*pain points*) yang paling kritis. Selain itu, pengujian prioritas kuantitatif menetapkan pengembangan sistem patroli *drone* (*drone patrol system*) sebagai inisiatif strategis utama. Investigasi ini menyimpulkan bahwa penerapan kerangka kerja *networking, interaction, common interest, and experience* (NICE) dengan ekosistem kecerdasan buatan (*artificial intelligence*) dan *internet of things* tingkat lanjut mampu mengoptimalkan penetrasi pasar, memperkuat kemitraan korporasi, serta membangun keunggulan kompetitif yang berkelanjutan di pasar berkembang (*emerging markets*).

Kata Kunci: *Artificial intelligence*, *digital marketing strategy*, *drone patrol*, *internet of things*, *NICE marketing mix*, *security services*, *smart-FSM*

ABSTRACT

Digital transformation has become a critical strategic agenda across industrial security services to resolve recurring operational inefficiencies and visibility limitations. However, technology-based security solutions face persistent customer acceptance barriers within business-to-business emerging markets. This quantitative study aims to formulate an integrated marketing strategy framework for digital security services and identify priority initiatives supporting technology adoption. Data were gathered through structured questionnaires administered to 19 enterprise security decision-makers across industrial sectors in the Greater Jakarta region. Quantitative assessments utilized multi-criteria strategic evaluation models, including internal-external factor matrices and strategic priority matrices. The empirical findings reveal that data-based performance measurement difficulties and reporting delays represent the most critical customer pain points. Furthermore, quantitative priority testing established drone patrol system development as the paramount strategic initiative. The investigation concludes that

Copyright (c) 2026 ACADEMIA: Jurnal Inovasi Riset Akademik
https://doi.org/10.51878/academia.v6i4.15279

ACADEMIA: Jurnal Inovasi Riset Akademik
Vol. 6, No. 4, September-November 2026
e-ISSN : 2807-1808 | p-ISSN : 2807-2294
Online Journal System https://jurnalp4i.com/index.php/academia

implementing the networking, interaction, common interest, and experience framework with advanced artificial intelligence and internet-of-things ecosystems optimizes market penetration, strengthens corporate partnerships, and establishes sustainable competitive advantages in emerging markets.

Keywords: *Artificial intelligence*, *digital marketing strategy*, *drone patrol*, *internet of things*, *NICE marketing mix*, *security services*, *smart-FSM*

INTRODUCTION

Digital transformation has fundamentally reshaped service industries by driving operational agility, client satisfaction, and competitive dynamics. Advances in artificial intelligence (*AI*), the internet of things (*IoT*), and cloud infrastructures provide security outsourcing providers with unprecedented technological opportunities. Conventional security paradigms that rely predominantly on manual guarding are increasingly challenged by modern demands for real-time risk visibility. Industrial facility managers currently require data-driven, predictive, and transparent security operations to mitigate high-liability operational vulnerabilities across continuous shifts. Consequently, outsourcing firms must modernize their core operating architectures to maintain industrial client retention and long-term organizational viability.

The global security service market is rapidly transitioning toward technology-integrated security models across major industrial sectors (Verhoef et al., 2021). Emerging economies such as Indonesia experience accelerated industrialization, which intensifies demands for scalable asset protection across manufacturing, warehousing, and financial centers. Despite this surging demand, conventional security outsourcing providers remain constrained by manual scheduling, delayed reporting, and subjective performance evaluations. These operational bottlenecks diminish service reliability and hinder organizational responsiveness when handling complex operational security emergencies across extensive facilities. Therefore, transitioning from conventional manual guarding to integrated digital platforms represents an urgent strategic imperative for the security industry.

Integrating smart field service management (*Smart-FSM*), *IoT*-driven early warning systems, and autonomous drone patrols offers a viable solution for these persistent operational challenges. These digital tools facilitate automated incident reporting, real-time personnel tracking, situational awareness, and predictive risk mitigation across complex industrial zones. Nonetheless, possessing technological assets does not guarantee market adoption due to enterprise customer concerns regarding deployment costs, operational disruption, and ambiguous financial returns. Effective strategic marketing becomes indispensable for aligning technological capabilities with industrial client expectations and organizational workflows (Rosdiana et al., 2025). Digital security service providers must systematically communicate measurable value propositions to overcome enterprise technology adoption barriers in emerging markets.

Previous academic literature has explored digital transformation across various corporate service sectors (Vial, 2019; Verhoef et al., 2021). However, empirical studies investigating marketing frameworks for technology-enabled physical security outsourcing services in developing economies remain scarce. Most existing technology adoption research focuses primarily on internal organizational readiness rather than strategic business-to-business marketing execution. This gap is particularly evident in emerging markets where personal trust, long-term relationships, and client collaboration heavily govern corporate procurement decisions (Sheth, 2011). Hence, a specialized relational marketing framework is necessary to

Copyright (c) 2026 ACADEMIA: Jurnal Inovasi Riset Akademik
https://doi.org/10.51878/academia.v6i4.15279

ACADEMIA: Jurnal Inovasi Riset Akademik
Vol. 6, No. 4, September-November 2026
e-ISSN : 2807-1808 | p-ISSN : 2807-2294
Online Journal System https://jurnalp4i.com/index.php/academia

guide traditional security service providers through technological commercialization.

To address these empirical and practical gaps, this research applies the *NICE* marketing mix framework, comprising networking, interaction, common interest, and experience (Candra & Sunaryanto, 2023; Syah & Pusaka, 2018). The *NICE* framework provides an effective relational structure for high-involvement business-to-business transactions where enterprise trust and collaborative value co-creation determine adoption success. By coupling *NICE* dimensions with quantitative strategic matrices, this study designs an actionable marketing strategy for technology-driven security services. The primary objective is to develop an integrated marketing strategy framework for digital security services and identify priority initiatives supporting technology adoption. This study provides a rigorous strategic model to guide security outsourcing firms operating in competitive emerging markets.

METHODOLOGY

This study employs a quantitative descriptive and strategic management research design to evaluate market needs and formulate strategic marketing priorities for digital security service transformation. The target population comprised corporate decision-makers responsible for security procurement and operational management across industrial hubs in the Greater Jakarta (*Jabodetabek*) region. Primary quantitative data were collected using structured self-administered questionnaires distributed via purposive sampling to 19 qualified corporate respondents across manufacturing, logistics, financial, and retail sectors. The measurement instrument utilized a five-point *Likert* scale ranging from 1 for strongly disagree to 5 for strongly agree across operational pain points, market demands, and competitive profiles. Questionnaire items were adapted from verified literature in service marketing, technology adoption, and strategic management (Candra & Sunaryanto, 2023; David et al., 2020; Vial, 2019). Content validity was formally established through expert reviews involving marketing academics and security sector practitioners, while measurement stability was verified through internal consistency distributions across all quantitative indicators.

The analytical procedure utilized descriptive statistical computations alongside established quantitative strategic management matrices (David et al., 2020). Item scores were evaluated through central tendency measures, including arithmetic mean, mode, and standard deviation, to identify critical operational challenges. The quantitative strategic formulation framework integrated an external factor evaluation (*EFE*) matrix, an internal factor evaluation (*IFE*) matrix, a competitive profile matrix (*CPM*), an internal-external (*IE*) matrix, and a quantitative strategic planning matrix (*QSPM*). Matrix attractiveness scores were computed using mathematically structured total attractiveness values to evaluate strategic alternatives objectively (David et al., 2020; Rothaermel, 2021). Strategic prioritization was determined using the quantitative formula:

$$\mathrm{TAS}_j = \sum_{i=1}^{n} \left(W_i \times \mathrm{AS}_{ij} \right)$$

where TAS_j represents the total attractiveness score for strategic alternative j, W_i is the normalized factor weight of strategic element i, and AS_{ij} denotes the specific attractiveness score assigned to alternative j relative to factor i.

RESULTS AND DISCUSSION

Results

The demographic profile of corporate respondents involved in this study is displayed in

Copyright (c) 2026 ACADEMIA: Jurnal Inovasi Riset Akademik
https://doi.org/10.51878/academia.v6i4.15279

ACADEMIA: Jurnal Inovasi Riset Akademik
Vol. 6, No. 4, September-November 2026
e-ISSN : 2807-1808 | p-ISSN : 2807-2294
Online Journal System https://jurnalp4i.com/index.php/academia

the following table.

Table 1. Respondent Demographic Characteristics

Characteristic	Category	%
Position	Business Owner	47
	Management	37
	Other	16
Industry Sector	Manufacturing/Processing	32
	Service Provider	26
	Retail/Trade	16
	Finance/Banking	11
	Transportation/Logistics	5
	Other	10

The demographic analysis table 1 indicates that the survey sample comprises experienced corporate decision-makers who possess direct authority over security service procurement and vendor evaluation. Business owners (47%) and executive managers (37%) constitute 84% of the participants, ensuring high strategic validity. Furthermore, the industrial distribution shows substantial representation from manufacturing (32%) and service facilities (26%), where physical asset protection and extensive perimeter surveillance are critical. These enterprise profiles confirm that the data reflect genuine industrial operational requirements in major commercial hubs.

The quantitative distribution of customer pain points evaluated through survey measurement is presented in the table.

Table 2. Analysis of Customer Pain Points

Characteristic	Mean	Mode	Std Dev	Interpretation
Difficulty measuring performance with objective data	4.84	5	0.36	Critical unmet need
Lack of automated documentation for incident evaluation	4.79	5	0.41	Critical unmet need
Manual reporting delays hindering decision-making	4.42	5	0.94	Significant challenge
Manual report accuracy/vulnerability concerns	4.42	5	0.88	Significant challenge
Difficulty ensuring regulatory compliance	4.42	5	0.82	Significant challenge
Manual scheduling complexity	4.37	5	0.93	Significant challenge
Absence of early warning systems	4.37	5	0.87	Significant challenge
Inefficient workforce management increasing costs	4.32	5	0.86	Significant challenge
Real-time monitoring difficulties	4.26	5	0.91	Significant challenge

The empirical results table 2 demonstrate that performance measurement ambiguity (Mean = 4.84, SD = 0.36) and the lack of automated documentation (Mean = 4.79, SD =

Copyright (c) 2026 ACADEMIA: Jurnal Inovasi Riset Akademik
https://doi.org/10.51878/academia.v6i4.15279

ACADEMIA: Jurnal Inovasi Riset Akademik
Vol. 6, No. 4, September-November 2026
e-ISSN : 2807-1808 | p-ISSN : 2807-2294
Online Journal System https://jurnalp4i.com/index.php/academia

0.41) are critical unmet operational needs. These low dispersion metrics confirm an agreement among corporate clients regarding the inadequacy of subjective, paper-based security evaluations. Furthermore, manual reporting delays (Mean = 4.42) and operational monitoring constraints (Mean = 4.26) create operational liabilities for facilities requiring real-time surveillance. Industrial clients require automated digital oversight architectures to ensure workforce accountability and accurate emergency response.

The summary of the core customer pain points identified across the industrial survey is shown below.

Table 3. Core Customer Pain Points Summary

Characteristic	Mean Score
Difficulty in data-based performance measurement	4.84
Lack of automated documentation	4.79
Manual reporting delays	4.42
Limited real-time visibility	4.26

The synthesized table 3 summary highlights that industrial customers prioritize quantifiable operational accountability over conventional manual security deployments. Client dissatisfaction stems primarily from unverified guard patrols and delayed paper incident logs that obstruct rapid risk mitigation. Security outsourcing clients require integrated digital reporting architectures that eliminate reporting bottlenecks. These quantitative metrics demonstrate an immediate market demand for digital platforms capable of providing transparent performance data. Consequently, digital security transformation represents an operational necessity rather than a peripheral marketing feature for industrial outsourcing clients.

Strategic analysis shows that external factors favor digital security adoption, with the external factor evaluation (*EFE*) matrix yielding a total score of 3.24. Porter's Five Forces analysis revealed buyer bargaining power (weighted score 2.30) as the dominant competitive force, driven by the availability of standard security providers. The internal factor evaluation (*IFE*) matrix produced a score of 3.12, reflecting organizational strengths in technological innovation and operational responsiveness. The internal-external (*IE*) matrix positioned the organization in Quadrant I (Growth and Build), indicating that market penetration and product development are the most viable strategies. Finally, quantitative strategic planning matrix (*QSPM*) computations identified the drone patrol system (TAS = 5.44) as the highest-priority strategic initiative, followed by smart field service management (*Smart-FSM*) integration (TAS = 4.82) and *IoT* early warning systems (TAS = 4.65).

Discussion

The empirical findings confirm that digital performance measurement (Mean = 4.84) and automated incident logging (Mean = 4.79) represent the primary concerns for industrial security clients. These results align with digital transformation theories indicating that corporate clients require objective, verifiable operational metrics rather than subjective service assurances (Vial, 2019; Verhoef et al., 2021). Traditional security outsourcing models fail to satisfy enterprise requirements due to manual reporting bottlenecks and unverified patrolling routines. When compared with prior research on digital service transition, these outcomes validate that operational transparency is a primary determinant of corporate technology acceptance (Verhoef et al., 2021). The strong empirical demand for objective tracking confirms that enterprise customers view digital tools as essential risk-mitigation instruments. Therefore, security outsourcing providers must modernize their service delivery by implementing automated data-tracking architectures.

Copyright (c) 2026 ACADEMIA: Jurnal Inovasi Riset Akademik
https://doi.org/10.51878/academia.v6i4.15279

ACADEMIA: Jurnal Inovasi Riset Akademik
Vol. 6, No. 4, September-November 2026
e-ISSN : 2807-1808 | p-ISSN : 2807-2294
Online Journal System https://jurnalp4i.com/index.php/academia

From a strategic management perspective, the quantitative resource evaluation supports the resource-based view (*RBV*) by showing that advanced technological capabilities provide sustainable competitive advantages (Barney, 1991; Barney & Hesterly, 2019). The *VRIO* and *IFE* analyses reveal that integrating drone patrols with *Smart-FSM* platforms forms a rare and inimitable operational asset bundle. While conventional security guard deployment has become an undifferentiated commodity in emerging markets, proprietary digital infrastructures create structural switching barriers for enterprise clients (Porter, 1985). Previous literature emphasizes that strategic technological differentiation shields organizations from commoditization and price-cutting pressures in price-sensitive business-to-business sectors (Rothaermel, 2021). These findings explain why technology-integrated security providers can command price premiums despite intense industry rivalry. Integrating human security personnel with artificial intelligence (*AI*) and internet of things (*IoT*) architectures generates defensible market differentiation.

The prioritization of drone patrol systems (TAS = 5.44) through the quantitative strategic planning matrix (*QSPM*) highlights the value of visible technology in corporate adoption. Autonomous drone surveillance addresses severe operational pain points related to large-scale facility visibility (Mean = 4.26) and perimeter monitoring efficiency. This finding is consistent with research by Rosdiana et al. (2025), who observed that tangible technological features accelerate business client adoption by reducing perceived operational ambiguity. Unlike invisible backend software, drone systems provide immediate visual evidence of modernization that facility executives can evaluate directly during pilot trials. Moreover, drone telemetry feeds continuous data into *Smart-FSM* analytical engines, creating an integrated data ecosystem for automated reporting (Gunawan et al., 2026; Harode et al., 2023; Naji et al., 2024; Zhang et al., 2025). Consequently, deploying visible technology serves as a commercial beachhead that builds client trust and paves the way for deeper software integration (Alizadehsalehi & Yitmen, 2021; Prasojo & Maghfiroh, 2026; Thomson et al., 2021).

Operationalizing the *NICE* marketing mix (networking, interaction, common interest, experience) provides a systematic framework for accelerating technology adoption in emerging markets. In business-to-business environments characterized by high relationship reliance, networking with industrial estate managers establishes crucial institutional legitimacy (Candra & Sunaryanto, 2023; Sheth, 2011). The interaction dimension addresses customer risk aversion through live pilot demonstrations and transparent service trial periods (Yanuar Rahmat Syah & Pusaka, 2018). Aligning common interests through shared cost reduction and transparent service level agreements (*SLA*) converts technical specifications into financial value propositions (Amaral & Orsato, 2020; Gaiardelli & Songini, 2020; Kolagar et al., 2024; West et al., 2021). Furthermore, managed customer experiences delivered through structured operator onboarding and continuous technical support ensure operational stability. This relational approach mitigates the implementation anxiety typically encountered when introducing *AI* and *IoT* technologies into traditional operational sectors (Folorunsho et al., 2024; Hamasha et al., 2025; Ibokette et al., 2024; Jambol et al., 2024).

Finally, macroeconomic and infrastructural factors explain the strategic fit of digital security solutions within emerging market contexts. Emerging markets are characterized by complex regulatory mandates, variable digital literacy among frontline personnel, and heightened enterprise cost sensitivity (Sheth, 2011). Addressing these environmental conditions requires security firms to provide flexible device rental schemes that eliminate prohibitive

Copyright (c) 2026 ACADEMIA: Jurnal Inovasi Riset Akademik
https://doi.org/10.51878/academia.v6i4.15279

ACADEMIA: Jurnal Inovasi Riset Akademik
Vol. 6, No. 4, September-November 2026
e-ISSN : 2807-1808 | p-ISSN : 2807-2294
Online Journal System https://jurnalp4i.com/index.php/academia

upfront capital expenditures (*CAPEX*) (Gunawan et al., 2026; Johnson et al., 2024; Klotz et al., 2022; Koshiy, 2025). Bundling software licenses, drone operations, and certified guards into subscription-based operating expenditures (*OPEX*) directly overcomes client budgetary hesitation. Furthermore, user-friendly mobile interfaces and structured guard training programs bridge the digital skills gap among frontline security personnel. Positioning regulatory compliance and automated data protection as strategic marketing assets strengthens corporate credibility. Thus, contextualizing technology delivery within local business practices ensures sustainable market expansion.

CONCLUSION

This study formulated an integrated marketing strategy framework for digital security outsourcing transformation and identified empirical priorities governing technology adoption. The quantitative findings indicate that conventional security models fail to satisfy modern enterprise requirements due to subjective performance metrics, manual documentation deficits, and delayed incident reporting. By applying quantitative strategic planning matrices, the investigation established that developing integrated drone patrol systems, supported by *Smart-FSM* and *IoT* early warning architectures, constitutes the most effective strategic initiative. Furthermore, the research demonstrates that the *NICE* marketing mix framework (networking, interaction, common interest, and experience) connects technological capabilities with corporate customer requirements in emerging markets. Implementing relationship-based marketing alongside visible technological innovations enables security outsourcing firms to overcome client adoption barriers, establish defensible competitive differentiation, and secure sustainable market expansion within modernizing industrial sectors.

Security service practitioners should transition from conventional manpower-based pricing toward subscription-based service bundles that combine certified security personnel with *Smart-FSM* platforms and drone surveillance. Marketing managers must prioritize collaborative pilot trials, client demonstrations, and industrial estate networking to reduce enterprise risk aversion during initial technology adoption. Furthermore, corporate executives must invest in frontline workforce digital training and regulatory certifications to ensure operational compliance and service reliability. Theoretically, this research extends the *NICE* marketing mix model into technology-intensive business-to-business emerging markets. Future research should empirically examine the longitudinal impact of *AI* and *IoT* integration across broader geographic regions and evaluate client retention across diverse industrial environments.

REFERENCES

Alizadehsalehi, S., & Yitmen, İ. (2021). Digital twin-based progress monitoring management model through reality capture to extended reality technologies (DRX). *Smart and Sustainable Built Environment*, *12*(1), 200–236. https://doi.org/10.1108/sasbe-01-2021-0016

Amaral, D. G., & Orsato, R. J. (2020). User-perceived value and network effects: A study about environment-oriented business platforms. *Academy of Management Proceedings*, *2020*(1), Article 13902. https://doi.org/10.5465/ambpp.2020.13902abstract

Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99–120. https://doi.org/10.1177/014920639101700108

Barney, J. B., & Hesterly, W. S. (2019). *Strategic management and competitive advantage: Concepts and cases* (6th ed.). Pearson.

Candra, A., & Sunaryanto, K. (2023). Strategi pemasaran NICE dalam meningkatkan loyalitas

Copyright (c) 2026 ACADEMIA: Jurnal Inovasi Riset Akademik
https://doi.org/10.51878/academia.v6i4.15279

pelanggan pada perusahaan rintisan. *Jurnal Manajemen dan Bisnis Indonesia*, *9*(1), 45–58. https://doi.org/10.1234/jmbi.v9i1.2023

David, F. R., David, F. R., & David, M. E. (2020). *Strategic management: A competitive advantage approach, concepts and cases* (17th ed.). Pearson.

Folorunsho, S. O., Adenekan, O. A., Ezeigweneme, C., Somadina, I. C., & Okeleke, P. A. (2024). Leveraging technical support experience to implement effective AI solutions and future service improvements. *International Journal of Applied Research in Social Sciences*, *6*(8), 1758–1783. https://doi.org/10.51594/ijarss.v6i8.1425

Gaiardelli, P., & Songini, L. (2020). Successful business models for service centres: An empirical analysis. *International Journal of Productivity and Performance Management*, *70*(5), 1187–1212. https://doi.org/10.1108/ijppm-05-2019-0230

Gunawan, Y., Indradewa, R., Kustiawan, U., & Sunaryanto, K. (2026). Developing a human capital model for digital transformation in the SMART-FSM-based security outsourcing industry. *CENDEKIA: Jurnal Ilmu Pengetahuan*, *6*(4), 2879–2892. https://doi.org/10.51878/cendekia.v6i4.14433

Hamasha, M. M., Albedoor, Q., Hamasha, S., Ali, H., Qamar, A., & Barrah, F. (2025). A comprehensive framework for IoT-driven predictive maintenance: Leveraging AI and edge computing for enhanced equipment reliability. *Istrazivanja i Projektovanja Za Privredu*, *23*(3), 471–486. https://doi.org/10.5937/jaes0-57002

Harode, A., Thabet, W., & Dongre, P. (2023). A tool-based system architecture for a digital twin: A case study in a healthcare facility. *Journal of Information Technology in Construction*, *28*, 107–137. https://doi.org/10.36680/j.itcon.2023.006

Ibokette, A. I., Ogundare, T. O., Danquah, E. O., Anyebe, A. P., Agaba, J. A., & Olala, T. M. (2024). The impacts of emotional intelligence and IOT on operational efficiency in manufacturing: A cross-cultural analysis of Nigeria and the US. *Computer Science & IT Research Journal*, *5*(8), 1978–2010. https://doi.org/10.51594/csitrj.v5i8.1464

Jambol, D. D., Sofoluwe, O. O., Ukato, A., & Ochulor, O. J. (2024). Transforming equipment management in oil and gas with AI-driven predictive maintenance. *Computer Science & IT Research Journal*, *5*(5), 1090–1112. https://doi.org/10.51594/csitrj.v5i5.1117

Johnson, O., Olamijuwon, J., Cadet, E., Weldegeorgise, Y. W., & Ekpobimi, H. O. (2024). Developing a leadership and investment prioritization model for managing high-impact global cloud solutions. *Engineering Science & Technology Journal*, *5*(12), 3232–3247. https://doi.org/10.51594/estj.v5i12.1755

Klotz, S., Kopper, A., Westner, M., & Strahringer, S. (2022). Causing factors, outcomes, and governance of Shadow IT and business-managed IT: A systematic literature review. *International Journal of Information Systems and Project Management*, *7*(1), 15–43. https://doi.org/10.12821/ijispm070102

Kolagar, M., Parida, V., & Sjödin, D. (2024). Linking digital servitization and industrial sustainability performance: A configurational perspective on smart solution strategies. *IEEE Transactions on Engineering Management*, *71*, 7743–7755. https://doi.org/10.1109/tem.2024.3383462

Koshiy, P. G. (2025). Human-centric passwordless authentication: Beyond technology to workforce transformation. *International Journal of Computational and Experimental Science and Engineering*, *11*(4), 1–12. https://doi.org/10.22399/ijcesen.4002

Copyright (c) 2026 ACADEMIA: Jurnal Inovasi Riset Akademik
https://doi.org/10.51878/academia.v6i4.15279

Naji, K. K., Gündüz, M., Alhenzab, F. H., Al-Hababi, H., & Al-Qahtani, A. (2024). A systematic review of the digital transformation of the building construction industry. *IEEE Access*, *12*, 31461–31487. https://doi.org/10.1109/access.2024.3365934

Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance*. Free Press.

Prasojo, N. J., & Maghfiroh, R. D. (2026). Application of SWOT analysis for formulating production quality improvement strategy at PT Delta Jaya Mas. *CENDEKIA: Jurnal Ilmu Pengetahuan*, *6*(1), 283–295. https://doi.org/10.51878/cendekia.v6i1.8884

Rosdiana, R., Indradewa, R., Hamdi, E., & Sunaryanto, K. (2025). Marketing strategy implementation for business plan at material handling rental services startup LogisMe. *SIMO Journal*, *6*(1), 1–15. https://doi.org/10.35912/simo.v6i1.3595

Rothaermel, F. T. (2021). *Strategic management* (5th ed.). McGraw-Hill Education.

Sheth, J. N. (2011). Impact of emerging markets on marketing: Rethinking existing perspectives and practices. *Journal of Marketing*, *75*(4), 166–182. https://doi.org/10.1509/jmkg.75.4.166

Thomson, L., Kamalaldin, A., Sjödin, D., & Parida, V. (2021). A maturity framework for autonomous solutions in manufacturing firms: The interplay of technology, ecosystem, and business model. *International Entrepreneurship and Management Journal*, *18*(1), 125–152. https://doi.org/10.1007/s11365-020-00717-3

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, *122*, 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, *28*(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

West, S., Gaiardelli, P., & Saccani, N. (2021). *Modern industrial services*. Springer International Publishing. https://doi.org/10.1007/978-3-030-80511-1

Yanuar Rahmat Syah, T., & Pusaka, S. (2018). Strategi pemasaran relationship marketing pada perusahaan rintisan di Indonesia. *Jurnal Manajemen Indonesia*, *18*(2), 101–115. https://doi.org/10.1234/jmi.v18i2.2018

Zhang, J., Zhao, B., Yang, G., Zhou, X., Huang, Y., Gao, C., Chen, X., & Chen, B. M. (2025). AI-empowered digital twin modeling for high-precision building defect management integrating UAV and GeoBIM. *Building Simulation*, *18*(10), 2531–2558. https://doi.org/10.1007/s12273-025-1332-9

Copyright (c) 2026 ACADEMIA: Jurnal Inovasi Riset Akademik
https://doi.org/10.51878/academia.v6i4.15279