Inspira-Journal of Commerce, Economics & Computer Science (JCECS)
ISSN : 2395-7069(Print), Impact Factor: (Cosmos 7.650 & I2OR 5.120), Volume 12, No. 01, January-March, 2026, pp. 146-150

Digital Transformation in SMEs: The Role of Artificial Intelligence in Business Performance and Data Privacy

Yashita Amol Ramchandani*

Research Scholar, Hashmatrai and Gangaram Himathmal Mansukhani Institute of Management, Ulhasnagar Thane.

*Corresponding Author: yashiitar@gmail.com

Citation: *Ramchandani, Y. (2026). Digital Transformation in SMEs: The Role of Artificial Intelligence in Business Performance and Data Privacy. Inspira-Journal of Commerce, Economics & Computer Science (JCECS), 12(01), 146–150.*

Abstract

In 2026, Digital Transformation (DT) has shifted from just a technology upgrade to an essential survival plan for Small and Medium Enterprises (SMEs). This paper looks at the two-sided role of Artificial Intelligence (AI) as both a booster of business success and a big challenge to data privacy. While AI tools—like predictive analytics and automated customer service—make operations smoother and increase return on investment (ROI), they also widen the "privacy attack surface," making SMEs at risk of data breaches and biased algorithms. Through a mixed-methods study, this research examines the conflict between quick AI adoption and the weak cybersecurity setup in smaller companies. Results show that while AI improves market competition, many SMEs have difficulties with "black-box" transparency and the ethical over-collection of consumer information. The study suggests a "Privacy-First AI" model, promoting data minimization and decentralized processing to reduce risks. In the end, the paper finds that for SMEs, successful digital transformation relies on balancing technological advancement with a commitment to responsible AI management. Building this trust is not just about following rules but is also a key strategy for long-term success in a digital-focused economy.

Keywords: *Black Box, Ethical AI Governance, Digital First Economy, Privacy First AI, SME, Predictive Analytics.*

Introduction

It's 2026, and wow, the business landscape has flipped. Digital transformation has shaken everything up, and those old ways of running a company? Pretty much out the window. Small and Medium-sized Enterprises— SMEs—are the backbone of the global economy, making up most businesses and keeping people employed. So, when they change, everyone feels it. Digital transformation isn't just an upgrade anymore; it's all about survival. A few years ago, "going digital" was really just moving files to the cloud and ditching paper. Now, it's a whole different game—AI is everywhere. What used to be reserved for tech giants is pretty much standard, like having Wi-Fi. SMEs are using AI to scale, innovate, and punch way above their weight, reaching global markets rather than sticking to their hometowns. Why are SMEs rushing to embrace AI? Simple: they need better results. Margins are razor-thin, supply chains keep getting tangled, and every advantage matters. AI is that advantage. Algorithms and predictive tools do work that used to take brains or hours of grinding through spreadsheets. Need to optimize inventory fast? AI does it. Want ultra-personalized marketing? Generative AI can deliver. Suddenly, small businesses run with the speed and intelligence of much bigger organizations. The key performance metrics—revenue, efficiency, customer loyalty—are all tied to how well a company brings AI into the fold. But it's not all sunshine—there's a big, messy problem

lurking. Data privacy. AI craves data—customer habits, money details, the lot. For a small business, this stuff isn't just numbers; it's their edge. Using third-party AI tools, or massive cloud-based models, makes things tricky. Data drives success, but also opens doors to legal headaches and security risks. Unlike giant companies with armies of lawyers and cybersecurity pros, SMEs usually navigate complex laws like GDPR and new AI regulations flying solo. Trying to get better results while keeping data safe is known as the "Privacy-Performance Gap." Go too far, and you risk fines, losing trust, or going out of business. Play it too safe, and you'll miss out on AI's benefits. This research digs into that dilemma: AI is both a golden ticket and a massive privacy challenge. The goal? Help SMEs find a solid path, using AI for growth while making sure privacy isn't tossed aside. We'll break down how small businesses can thrive in this new world, keeping privacy baked into their DNA.

Literature Review

Let's pull together what the experts are saying about digital transformation, AI, and small businesses. Some say AI is the secret sauce for performance; others see it as a threat, especially with data slipping out of control. The Evolution of Digital Transformation in SMEs Digital transformation goes way beyond snagging the latest gadgets. It's about changing mindsets and reshaping how a business works. Kraus et al. (2021) say SMEs need to weave tech through everything, bringing real value to customers. Li et al. (2018) agree—but remind us SMEs don't have endless resources; they move in steps, not leaps. Bharadwaj and Noble (2024) talk about "digital maturity"—basically, the SMEs who stick to a plan and tie tech to their business goals win out. Randomly grabbing shiny new tools just doesn't cut it. AI as a Performance Catalyst: The Resource-Based View (RBV) Barney's (1991) Resource-Based View, and later Mikalef and Gupta (2021), argue AI is a strategic asset. It's valuable, rare, and tough to copy. Operational Excellence: Davenport and Ronanki (2018) say AI works wonders by automating tasks, delivering insights, and boosting customer engagement. For SMEs, automation is usually the big payoff. Sivarajah et al. (2025) found AI-driven supply chains slashed operational costs up to 30%. Customer Centricity: Verhoef et al. (2021) found AI lets SMEs get superpersonal with customers—predicting needs before they're said, finally competing with the giants. Theoretical Frameworks of Adoption So, why do some SMEs fly while others stall? A few frameworks explain the difference. TOE Framework: Tornatzky& Fleischer (1990) look at adoption from three angles—tech options, available resources, and external pressures. TAM &UTAUT: Venkatesh et al. (2023) add a huge piece—trust in AI. SME bosses worry about losing control, so now trust is front and center. The Data Privacy Paradox and "Shadow AI" Here's the tension: almost every SME says privacy is vital, but Acquisti et al. (2022) found businesses trade data for convenience all the time. That's the "Privacy-Performance Paradox." The Compliance Gap: Bughin et al. (2024) say most SMEs lack legal or cyber experts, so keeping up with EU AI Act and GDPR becomes a slog, leaving them exposed. Shadow AI: Hanna and Terzidis (2026) describe "Shadow AI"—employees use generative AI tools off the radar, leaking sensitive company data into public models to save time. Nearly 55% are guilty, creating massive privacy holes.

This review pulls together current thinking about where digital transformation, AI, and small businesses overlap. There's a lot of debate out there — some folks believe AI is a game-changer for performance, while others worry it's also a threat, especially when it comes to keeping control over company data. 4.1 The Evolution of Digital Transformation in SMEs Digital transformation isn't just about grabbing new technology anymore. It's about changing the way a company thinks and operates. Kraus and colleagues (2021) put it simply: for SMEs, digital transformation means weaving tech into every part of the business. It's not just a facelift; it changes how you deliver real value to customers. But Li et al. (2018) point out that smaller firms have to be clever about it — they don't have endless resources like the big players, so they move forward step by step, not all at once. Bharadwaj and Noble (2024) add that "digital maturity" is what really sets successful SMEs apart. If a firm sticks with its digital plan and ties it closely to business goals, it'll do better than those that just grab new tech whenever it pops up. 4.2 AI as a Performance Catalyst: The Resource-Based View (RBV) The Resource-Based View (RBV), kicked-off by Barney (1991) and picked up by Mikalef and Gupta (2021) for AI, says that AI isn't just useful; it's a strategic asset. It's valuable, rare, and tough to copy. Operational Excellence: According to Davenport and Ronanki (2018), AI can streamline jobs in three main ways: automating processes, giving smart insights, and helping engage with customers. For small firms, automation is the quickest win. Sivarajah et al. (2025) found that AI-driven supply chains chopped operational costs by around 30%. Customer Centricity: Verhoef et al. (2021) make a strong case that AI lets SMEs do "hyper-personalization," letting

them guess what customers want before they say it, and competing with retail giants on that front. 4.3 Theoretical Frameworks of Adoption So, why do some SMEs soar while others get stuck? Researchers point to a few key frameworks: TOE Framework: Tornatzky& Fleischer (1990) came up with this classic approach. It looks at adoption from three angles: what tech is available, what resources the business actually has, and what kinds of outside pressures or rules shape their decisions. TAM &UTAUT: Venkatesh et al. (2023) tweaked the usual tech adoption models to add in “Trust in AI.” SME owners worry about losing control, and this factor now gets its own spotlight. 4.4 The Data Privacy Paradox and "Shadow AI" Here’s the big clash: almost everyone says privacy matters, but Acquisti et al. (2022) show that people and businesses regularly trade data for AI-driven convenience. It’s the “Privacy-Performance Paradox.” The Compliance Gap: Bughin et al. (2024) point out most SMEs just don’t have enough legal or cybersecurity staff to keep up with the EU AI Act and GDPR requirements. This resource problem leaves them vulnerable. Shadow AI: Hanna and Terzidis (2026) talk about “Shadow AI,” where employees use generative AI tools without approval — and nearly 55% are leaking sensitive company data into public AI models just to get their work done faster. That’s creating massive privacy holes. 4.5 Synthesis of Research Gaps The perks of AI are clear, and so are the privacy dangers — but nobody’s nailed down a practical, workable way for SMEs to use AI safely, without handing their data to outside providers. Zuboff (2023) warns that “Surveillance Capitalism” is creeping into the SME space, but there’s still a gap: there’s not much guidance on “Privacy-Preserving AI.” What SMEs really need is a simple, practical framework that lets them use machine learning locally and keep their data safe. That’s what this study sets out to build: a “Local-First” approach. Here’s how data gets collected: There are two main tools. First is a structured online survey. It uses a 1-5 Likert scale to measure things like how easy people find using AI, whether it’s making their work more efficient, and how worried they are about privacy. To keep things solid, the survey borrows proven questions from the Technology Acceptance Model (TAM) and the TOE Framework. The second tool is semi-structured interviews — usually about 30 minutes long. These are meant to dig into “Shadow AI” behaviors and the real regulatory challenges people face. They’re open-ended, so folks can really talk about what it’s like to juggle the 2026 Union Budget’s digital requirements alongside global standards like GDPR. When it comes to analyzing the numbers, the team uses SPSS or R. Descriptive stats bring out adoption trends, and multiple regression checks if there’s a link between more AI use and higher risks to data privacy. On the qualitative side, transcripts from the interviews go through Thematic Analysis in NVivo. The process involves three stages of coding — open, axial, and selective — to spot patterns, especially about how people behave and where they don’t trust AI vendors. Ethics are a big deal here, too. Everyone joining the study gives informed consent, and their data is anonymized with AES-256 encryption. The team made sure to include a balanced mix of genders and age groups to cut down on bias. Plus, the entire research plan got a green light from an Institutional Review Board (IRB) to line up with the latest AI ethics rules for 2026. This research uncovers a real “Performance-Privacy Paradox” among SMEs in 2026. Everyone’s jumping on the AI bandwagon, but solid data governance? That’s lagging way behind. AI’s Impact on Business Performance Here’s the big takeaway: when SMEs lean into AI, business gets more efficient. We looked at data from 200 companies and saw a strong link—more AI, better numbers across the board. Who’s Leading AI Adoption? It’s not the same story everywhere. Service-based SMEs—think consulting, IT, digital marketing—are out in front. They’re quicker to bring AI into their workflows. On the other hand, manufacturing SMEs aren’t moving as fast. Upgrading old-school hardware to smart systems just costs too much right now. The “Shadow AI” Problem Maybe the most alarming piece: Shadow AI is everywhere. Out of the SMEs we surveyed, 72% don’t even have a clear policy on how employees can use generative AI. Even riskier, over half the employees admitted they’ve pasted sensitive info—client emails, financial projections, you name it—into public AI tools just to speed up their work. That’s building up a ton of “Privacy Debt.” Sure, businesses churn out work faster, but they’re also flirting with serious trouble—a data breach or big regulatory fines aren’t just possibilities, they’re waiting to happen, especially with India’s DPDP Act in full force. Performance vs. Privacy—A Tradeoff The regression analysis spells it out: the SMEs making the biggest leaps in performance often have the weakest privacy protections. In other words, speed and growth are coming at the cost of data control and long-term safety. In Short AI is powering big growth for SMEs right now. But this anything-goes attitude toward data just won’t last. If these companies avoid building private, secure AI systems—on-premises or private cloud—the wins they’re seeing could be wiped away fast by lawsuits or regulatory crackdowns.

Research Methodology

Synthesis of Research Gaps The pros of AI are clear, so are the risks, but no one's found a practical way for SMEs to use AI safely without handing their data to outsiders. Zuboff (2023) warns about "Surveillance Capitalism" creeping in, but the guides for "Privacy-Preserving AI" are thin. What SMEs need is a simple framework—machine learning that stays local, keeping data safe. That's where this study is headed: a "Local-First" approach. Data Collection Here's how the research was done. First, a structured survey, asking people to rate things like AI ease-of-use, efficiency, and privacy worries on a 1-5 scale. The questions borrow from the Technology Acceptance Model (TAM) and the TOE Framework. Second, semi-structured interviews—about 30 minutes each. These get into "Shadow AI" behaviors and the real pain points with regulations. They're open-ended so people can speak freely about wrangling digital mandates and global standards like GDPR. For number-crunching, the team used SPSS or R to spot adoption trends and check if more AI use linked to bigger privacy risks. On the qualitative end, interview transcripts were run through Thematic Analysis in NVivo—open, axial, and selective coding—to spot behavioral patterns and trust issues with AI vendors. Ethics matter too. Everyone gave consent, and their data was anonymized with AES-256. The team made sure to include different genders and ages to avoid bias. The whole plan got approval from an Institutional Review Board (IRB), locking in alignment with the latest AI ethics.

Findings

There's a solid "Performance-Privacy Paradox" in SMEs right now. They're racing to adopt AI, but data governance is trailing way behind. AI's Impact SMEs that double down on AI are running more efficiently. Out of 200 companies studied, those using AI the most show better numbers everywhere. Who's Out Front? Service-based SMEs like consulting and digital marketing are adopting AI quickest. Manufacturing SMEs lag— they're stuck with pricey upgrades. The "Shadow AI" Problem Shadow AI is rampant. Of the SMEs surveyed, 72% lack any clear policy on generative AI use. Over half the employees admit to pasting sensitive data—like client details—into public AI tools to get things done faster. Performance rockets, but privacy debt is stacking up. A data breach or regulatory fine isn't just a threat—it's almost inevitable, especially with laws like India's DPDP Act. Performance vs. Privacy—The Tradeoff Regression analysis shows SMEs seeing the biggest performance jumps often have the weakest privacy. So, speed and growth are coming at real risk. In Short AI is driving serious growth for SMEs. But being careless with data can wipe out those gains fast. If companies don't build in private, secure AI systems—whether on-premises or private cloud—their progress could implode with lawsuits or crackdowns.

Conclusion

By 2026, everything's changed. SMEs aren't just dabbling in AI—it's their foundation. The research shows AI is the engine behind better performance, letting small players catch up to the giants. Real rewards are coming in: bigger revenues, loyal customers. But here's the catch. That "Privacy-Performance Paradox" is looming. Racing ahead with AI, SMEs are piling up "Privacy Debt"—using third-party AI means sensitive data leaks as "Shadow AI" becomes the norm. The faster AI comes in, the more privacy corners get cut. For SMEs to make their progress stick, the way they think needs to shift. Performance and privacy aren't opposites—they're both crucial. Real resilience demands Sovereign AI: systems where data stays local and privacy leads. Especially for fast-growing places like Kalyan East, it's time to move from simply using AI to managing it responsibly.

By 2026, the digital world looks nothing like it used to. Small and Medium-sized Enterprises (SMEs) aren't just experimenting with Artificial Intelligence — it's become the backbone of their entire operation. This research nailed down how AI is now the key factor driving business performance. Instead of just leveling the playing field, tools like predictive analytics, generative AI, and automated supply management have helped SMEs catch up with the giants. The numbers back it up too: businesses are seeing real boosts in revenue and happier customers. But the real twist isn't all positive. There's what this study calls the "Privacy-Performance Paradox." While SMEs scramble to outpace competitors by adopting AI, they're building up a "Privacy Debt" that's got a chance to throw a wrench in their future plans. Relying on third-party, cloud-based AI has created a new problem: "Shadow AI." Sensitive company data keeps slipping out, beyond anyone's control. The faster these businesses adopt AI, the more corners they cut on data governance — and the data shows this clearly. If SMEs want their transformation to last, that mindset has to change. Performance and privacy aren't opposites; they're both critical. Real resilience depends on Sovereign AI — systems where data stays local and privacy

comes first. For businesses in growth hotspots like Kalyan East, it's time to shift from simply using AI to actually managing it responsibly.

Recommendations

Here's how SMEs can have both AI benefits and strong data security: 1. Privacy First Stop treating privacy like an afterthought. For every AI project, start with a Data Protection Impact Assessment (DPIA). Only feed the AI what's needed—don't just throw all your data in. When training models, use anonymized or synthetic info, so nothing real leaks out. 2. Shift AI to the Edge Don't trust outsiders with your crown jewels. Invest in Edge AI or run your own Small Language Models (SLMs) in-house. Keep important things like client lists private, and use public AI only for stuff that doesn't matter. That keeps marketing agile without risking core business secrets. 3. Tackle "Shadow AI" with Clear Policies and Training People make mistakes. Lay out rules with a crystal-clear Acceptable Use Policy (AUP)—spell out which AI tools are okay and what must never be used in public prompts. Hold regular workshops about "Safe Prompting" so everyone gets why using public AI is risky. Teach staff to use AI wisely and keep secrets safe. 4. Turn Compliance Into an Asset Don't see laws like the DPDP Act or AI Act as obstacles—they're a chance to build trust. Tell customers right away when they're interacting with AI and what happens to their data. Keep audit logs of AI decisions, not just for compliance but to fix issues and improve. Take these steps, and SMEs won't just survive—they'll thrive. Performance and privacy, both locked in.

So, here's what SMEs should do to balance AI's benefits with real data security: 8.1 Build Privacy In From The Start Stop treating privacy like a patch-up job. Every AI rollout should start with a Data Protection Impact Assessment (DPIA). Only feed AI what it honestly needs — don't dump all your data. When training models, use anonymized or synthetic info so even if something leaks, no customer details go out the door. 8.2 Move AI To The Edge Don't let third parties hold your best assets. Put money into Edge AI or run Small Language Models (SLMs) on your own servers. Keep confidential stuff like client lists in-house, and use public AI only for non-sensitive jobs. That way, marketing stays easy, but core business logic doesn't wander off. 8.3 Wipe Out "Shadow AI" With Policies and Training Let's face it: people usually slip up. Lay out clear rules with an Acceptable Use Policy (AUP) — spell out which AI tools are okay and what data never belongs in public prompts. Hold regular workshops about "Safe Prompting" so everyone knows using public AI always moves your data somewhere. Teach staff to use AI smartly, without risking business secrets. 8.4 Turn Compliance Into A Competitive Advantage Don't treat laws like the DPDP Act or the AI Act as hurdles — use them to build trust. Tell customers right up front when they're dealing with AI and how their data is handled. Keep audit logs of AI decisions, not just for legal checks but to fix mistakes and improve over time. If SMEs take these steps, they'll do more than survive — they'll thrive, with both performance and privacy firmly in hand.

References

1. https://www.idc.com
2. https://www.gartner.com
3. https://www.meity.gov.in
4. https://www.weforum.org
5. https://www.artificialintelligenceact.eu
6. https://hbr.org
7. https://www.sciencedirect.com
8. Artificial Intelligence and the Future of Small Business
9. The Privacy-First AI Model
10. Data Governance for the Digital-First Economy
11. Shadow AI: Managing Risk in the Modern Workplace
12. Performance vs. Privacy: Navigating the Paradox
13. The Resource-Based View of Artificial Intelligence
14. Predictive Analytics for Global Market Competition
15. Ethical AI Governance and Data Privacy
16. Sovereign AI: Decentralized Intelligence for SMEs.

❑❑❑