2.4.2. 2025-2026 年最新技術轉向與安全防護趨勢

針對中小企業在導入生成式人工智慧（GenAI）時所面臨的資訊安全與機密外洩挑戰，學術界在防護路徑的探討上呈現出顯著的演進。透過對比 2025 年與 2026 年的最新文獻，可發現研究視角已從「強調合規與成本困境的被動防禦」轉向「運用低成本技術架構進行主動防禦」的務實路徑。以下針對學術界在 AI 安全防護技術上的最新轉向進行深度分析：

1. 2025 年的觀點：陷入資源匱乏與高昂防護成本的矛盾困境 回顧 2025 年的文獻，學術界主要聚焦於中小企業在確保資訊安全與符合嚴格法規（如 GDPR）時所面臨的財務與技術雙重屏障。研究指出，企業在進行商業分析時，若將專有敏感數據傳送至外部大型語言模型（LLMs）的應用程式介面（APIs），將引發嚴重的隱私與數據主權風險（Salazar & Kunc, 2025）。然而，為防範此類風險所提出的高規格解決方案（如部署大型私有化地端模型、建立嚴格的資安防火牆或客製化模型訓練），對多數中小企業而言過於昂貴且難以實行（Bran et al., 2025; Carayannis et al., 2024）。在此階段，由於缺乏足夠的研發預算與資安基礎設施，中小企業往往只能仰賴脆弱的行政管理手段（如明文禁止員工輸入機密資訊），在防護上處於被動且充滿漏洞的狀態。

2. 2026 年的最新轉向：本地小型模型與 **RAG** 架構的技術突圍 相對於 2025 年對成本與合規困境的宏觀描述，2026 年的最新研究在安全防護技術路徑上出現了明確的轉向。研究證實，員工將敏感資料輸入雲端公共模型不僅違反隱私法規，更會造成數據控制權喪失的「不可逆」風險，且擴大了企業面臨提示注入（Prompt-injection）等攻擊的受攻擊面（Leonard et al., 2026）。為徹底解決此一痛點，學術界提出了符合中小企業資源限制的最新技術防護趨勢：

- 轉向部署規模較小且可內部管理的本地模型（**Local Models**）：Leonard et al. (2026) 明確指出，既然中小企業難以負擔從頭訓練大型私有模型的龐大成本，AI 防護的創新與實踐正轉向部署規模較小、計算資源需求較低，且可完全由企業內部 IT 環境控管的本地模型。此一路徑讓企業在不依賴外部第三方雲端算力的情況下，重新掌握核心技術的控制權。
- 運用 **RAG** 架構落實數據主權保護（**Data Sovereignty**）：在本地模型的基礎上，最新研究強烈建議中小企業採用檢索增強生成（**Retrieval-Augmented Generation, RAG**）架構 作為資料防護的核心技術。Leonard et al. (2026) 強調，RAG 技術允

許企業將專有的商業機密文件保存在本地端或受控的存儲空間中。當模型運行時，是透過檢索本地知識庫來生成精準答案，而非將機密數據上傳至外部公共模型進行重新訓練。顯見，RAG 架構有效隔離了內部敏感數據與外部雲端網路，從根本上阻斷了機密外洩的途徑，成為中小企業在有限資源下，實現數據主權保護與安全應用 AI 的最可行技術轉向。

總結而言，2025 年至 2026 年間的文獻發展展現了清晰的技術演進時間軸：從早期擔憂大型私有模型成本過高，轉向提倡運用「本地小型模型結合 RAG 架構」來打造專屬的資料安全護城河。此一技術轉向不僅消弭了中小企業資源匱乏與高昂資安成本之間的矛盾，更為保護企業數據主權提供了具體且可落地的實務解方。

參考文獻

Bran, F., Bodislav, D. A., Călin, A. M., & Mănescu, A. M. (2025). Empowering SMEs through Generative AI: Opportunities, Challenges, and Strategic Implications for Sustainable Innovation. *European Journal of Sustainable Development*, 14(4), 27-38.

Carayannis, E. G., Dumitrescu, R., Falkowski, T., & Zota, N.-R. (2024). Empowering SMEs: Harnessing the Potential of Gen AI for Resilience and Competitiveness. *IEEE Transactions on Engineering Management*, 1-13.

Leonard, E., Sheehan, B., Mullins, M., & Shannon, D. (2026). Generative AI for enhanced risk management in SMEs. *Journal of Risk Research*, 1-22.

Salazar, A., & Kunc, M. (2025). The contribution of GenAI to business analytics. *Journal of Business Analytics*, 8(2), 79-92.