



10 XU HƯỚNG CÔNG NGHỆ TẠI VIỆT NAM 2026

Cơ hội tăng tốc trong làn sóng
công nghệ toàn cầu

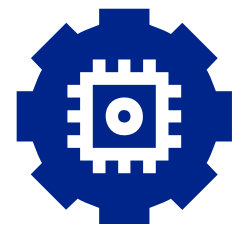
FPT Smart Cloud, Tập đoàn FPT – Tháng 2/2026



Bối cảnh công nghệ toàn cầu 2026	3
Bức tranh công nghệ Việt Nam	4
10 xu hướng công nghệ nổi bật tại Việt Nam 2026	5
1. Multi-agent Systems	6
2. AI-native Development Platforms	8
3. AI Factory – Computing Infrastructure for AI	10
4. Domain-specific Language Models (Vertical LLMs)	12
5. AI Governance & AI Security Platforms	14
6. Preemptive Cybersecurity	16
7. Computer Vision & Vision Agents	18
8. Physical AI	20
9. Digital Provenance & Content Integrity	22
10. Quantum Computing	24
Bước tiếp theo cho doanh nghiệp	26

Bối cảnh công nghệ toàn cầu 2026

Năm 2026, AI chuyển sang giai đoạn vận hành ở quy mô lớn. Cuộc chơi giữa các doanh nghiệp sẽ nằm ở 3 trụ cột: **Hạ tầng cloud – Bảo mật – Quản trị.**



Đầu tư công nghệ mang tính hệ thống

Theo Gartner dự báo chi tiêu cho Công nghệ thông tin toàn cầu sẽ **tăng 9,8%**, lần đầu tiên vượt mức **6 nghìn tỷ USD⁽¹⁾**, riêng **tổng chi tiêu AI toàn cầu năm 2026 đạt ~2.52 nghìn tỷ USD⁽²⁾**. Các doanh nghiệp đầu tư trải đều vào nhiều mảng như dữ liệu, nền tảng, bảo mật, hạ tầng...



AI Agents: Lực lượng lao động số mới

Gartner dự báo đến 2029, **Agentic AI** sẽ tự xử lý 80% vấn đề dịch vụ khách hàng, giảm 30% chi phí vận hành⁽³⁾. Các **Agents** chuyên biệt hóa theo nhiệm vụ và được quản lý bằng cơ chế định danh, phân quyền, kiểm soát dữ liệu nghiêm ngặt như một nhân sự thực thụ.



Sự bùng nổ của xưởng sản xuất phần mềm

GitHub ghi nhận **~43 triệu pull requests/tháng** (tăng **23% YoY**) và **khoảng 1 tỷ commits/năm⁽⁴⁾**, báo hiệu một sự chuyển đổi lớn trong ngành, khi AI trực tiếp tham gia vào cách thức xây dựng và cải tiến phần mềm, thúc đẩy chu kỳ đổi mới sáng tạo diễn ra nhanh hơn bao giờ hết.



Chủ quyền số: Điều kiện để mở rộng quy mô

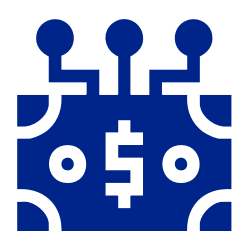
Theo IBM, **93% lãnh đạo cho biết AI có chủ quyền (AI Sovereignty)** sẽ là “bắt buộc” trong chiến lược doanh nghiệp năm 2026⁽⁵⁾. Chủ quyền AI bao gồm kiểm soát mô hình và bảo mật dữ liệu, giúp doanh nghiệp triển khai AI trên diện rộng, an toàn, bền vững.



Thông điệp: AI sẽ trở thành công nghệ đồng hành giúp doanh nghiệp triển khai vận hành một cách **An toàn hơn – Kiểm soát tốt hơn – Vận hành bền vững hơn.**

Bức tranh công nghệ tại Việt Nam

Năm 2026, thị trường Việt Nam hội tụ đủ “lực kéo” để đưa AI từ thử nghiệm vào vận hành thực tế. Trọng tâm chiến lược chuyển dịch là tối ưu hóa dữ liệu, đảm bảo an toàn hệ thống và triển khai AI đúng mục tiêu.



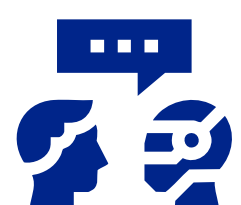
Nền kinh tế số bùng nổ quy mô

Kinh tế số Việt Nam duy trì đà tăng trưởng ấn tượng với tổng giá trị hàng hóa (GMV) đạt **72,1 tỷ USD** (2025), tăng trưởng 14.6%⁽⁶⁾. Sự lớn mạnh về quy mô tạo ra nhu cầu cấp thiết về việc tự động hóa vận hành thông minh.



Thanh toán số: Động cơ tăng trưởng chính

Thanh toán số đóng vai trò là “mạch máu” và giữ đà tăng trưởng mạnh khi Chính Phủ đẩy mạnh việc thanh toán không dùng tiền mặt, thúc đẩy các giải pháp AI phát huy khả năng trong đối soát, bảo mật và quản trị rủi ro tài chính.



Người dùng sẵn sàng tương tác với AI Agents

Theo Vietnam e-economy SEA 2025, 81% người dùng tương tác với AI hàng ngày, trong đó, 96% sẵn sàng chia sẻ dữ liệu cho AI để được cá nhân hóa trải nghiệm⁽⁷⁾. Điều này đặt ra áp lực phải xây dựng các bộ giải pháp ứng dụng AI đảm bảo an toàn, minh bạch.



Động lực từ Chính phủ & Pháp lý

Nhà nước đẩy mạnh chuẩn hóa dữ liệu quốc gia và thiết lập khung pháp lý mới. Luật Trí tuệ nhân tạo đã được Quốc hội thông qua và có hiệu lực từ **01/03/2026**⁽⁸⁾ sẽ tạo nền tảng quản trị rủi ro, thúc đẩy thử nghiệm có kiểm soát và triển khai AI ở quy mô lớn, an toàn hơn.



Thông điệp: Để hiện thực hóa AI tại Việt Nam, doanh nghiệp cần giải quyết ba bài toán trụ cột: **Dữ liệu tin cậy - Bảo mật tuân thủ - Hạ tầng Cloud linh hoạt.**

Xu hướng công nghệ nổi bật 2026

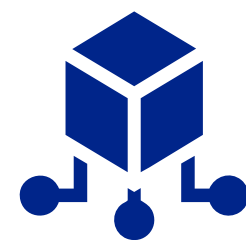
Câu hỏi chiến lược của các doanh nghiệp sẽ tập trung vào tính thực thi:
Triển khai AI vào quy trình thực tế như thế nào? Khả năng mở rộng ra sao? Và Làm thế nào để kiểm soát rủi ro?

3 tiêu chí định hình các xu hướng công nghệ 2026:



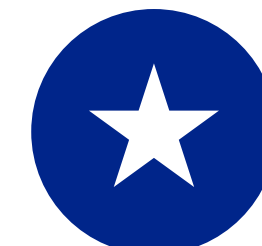
Tác động kinh doanh định lượng

Phải tạo ra giá trị đo lường được thông qua việc tăng năng suất, tối ưu chi phí hoặc nâng tầm trải nghiệm khách hàng.



Nền tảng vận hành bền vững

Dựa trên sự hội tụ của Điện toán đám mây (Cloud), Bảo mật (Security) và Quản trị (Governance).



Tính khả thi tại thị trường Việt Nam

Khả năng triển khai thực tế trong vòng 12–24 tháng nhờ lực kéo từ kinh tế số và hành vi người dùng nội địa.



Càng đẩy mạnh "AI hóa", doanh nghiệp càng phải thực hiện song song:
Tăng tốc đổi mới đi kèm **thắt chặt tiêu chuẩn kiểm soát** về định danh, phân quyền, truy vết và bảo vệ dữ liệu.



PGS.TS Ngô Xuân Bách

Giám đốc Khối Sản phẩm AI,
FPT Smart Cloud;

Giám đốc Viện Nghiên cứu Quantum AI
& Cyber Security, Tập đoàn FPT

1 Multi-agent Systems

Multi-agent Systems là gì?

Multi-agent Systems (MAS) là hệ thống gồm nhiều nhân sự AI, tương tác với nhau trong một môi trường chung, để giải quyết các nhiệm vụ phức tạp mà một agent đơn lẻ thực hiện không hiệu quả, bằng cách phân chia công việc, xử lý song song, học hỏi và thích ứng tập thể.

Agents vận hành theo nhiệm vụ, từ lập kế hoạch, gọi công cụ, truy cập hệ thống (ERP/CRM) và phối hợp theo luồng công việc để tạo ra kết quả thực tế.

Tiềm năng phát triển

MAS sẽ bùng nổ tại Việt Nam bởi 3 nguyên nhân:

- **Áp lực quy mô kinh tế số:** Đòn bẩy giúp doanh nghiệp tự động hóa toàn diện chuỗi giá trị, từ logistics đến thanh toán.
- **Tối ưu năng suất gắn liền với Chủ quyền dữ liệu:** Cho phép thiết lập quy trình tự động hóa có kiểm soát, đáp ứng các tiêu chuẩn bảo mật khắt khe.
- **Hệ sinh thái AI quốc gia:** Tạo môi trường lý tưởng để triển khai AI, hiện thực hóa chiến lược lọt Top 50 thế giới về AI vào 2030⁽⁹⁾.

Ứng dụng thực tế



Ngân hàng – Bảo hiểm

Phối hợp agent "Trợ lý nghiệp vụ" và agent "Chống gian lận" để truy vết giao dịch...



Logistics – Sản xuất

Phối hợp với agents lập kế hoạch sản xuất, bảo trì dự đoán và tối ưu hóa tuyến vận hành...



Bán lẻ – Thương mại điện tử

Agents tối ưu chiến dịch Marketing, dự báo nhu cầu, chăm sóc khách hàng đa kênh...



Dịch vụ công

Agents phân luồng hồ sơ, kiểm tra tuân thủ, giúp tăng minh bạch và giảm công việc thủ công...

Góc nhìn doanh nghiệp

MAS là "hệ điều hành mới" cho doanh nghiệp số, chuyển từ các AI đơn lẻ sang đội ngũ AI Agents. Tại FPT, FPT.AI là đơn vị cung cấp giải pháp MAS toàn diện, giúp doanh nghiệp xử lý các nghiệp vụ thực tế.

Lớp điều phối
(Orchestration)

Quản lý sự phối hợp phức tạp giữa nhiều agents.

Tích hợp hệ thống lõi

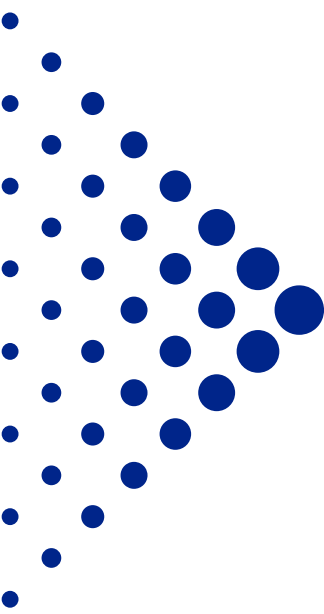
Kết nối trực tiếp qua API với CRM, ERP, ITSM sẵn có.

Vận hành chuẩn doanh nghiệp

Tích hợp sẵn Giám sát, Quản trị, Kiểm soát chi phí và Truy vết.

Để MAS vận hành trong môi trường dữ liệu nhạy cảm, chúng tôi tập trung vào

5 trụ cột hạ tầng và bảo mật:



- 1 **Hạ tầng tính toán:** Tối ưu hóa cho cả huấn luyện (Training) và suy luận (Inference).
- 2 **Quản trị truy cập (IAM):** Kiểm soát tuyệt đối phạm vi tiếp cận dữ liệu của agent.
- 3 **Khung quản trị rủi ro:** Đảm bảo tính tuân thủ cho các ngành có rào cản pháp lý cao.
- 4 **Điều phối liên hệ thống:** Kết nối agent với hệ thống lõi qua API và luồng công việc để tự động hoá từ đầu đến cuối.
- 5 **Bảo mật thời gian chạy cho agent:** Thiết lập hàng rào an toàn, cơ chế phê duyệt và giám sát những hành động nhạy cảm trên hạ tầng Cloud.

Khuyến nghị trước khi triển khai

- ✓ **Chuẩn hóa quyền hạn:** Định danh và giới hạn quyền truy cập cho agents theo nguyên tắc rõ ràng.
- ✓ **Tách lớp điều phối và các bước hành động:** Kiểm soát, ghi nhật ký (Log/Audit) và phê duyệt các hành động quan trọng.
- ✓ **Đo lường theo mục tiêu kinh doanh:** Thiết lập KPI về thời gian xử lý, tỷ lệ lỗi, mức độ tuân thủ và kiểm thử các tình huống tấn công.

Thông điệp



“Để thành công với MAS, doanh nghiệp không chỉ nhìn vào công nghệ, mà dựa vào cách quản trị một đội ngũ nhân sự số. FPT.AI cung cấp bộ giải pháp FPT AI Agents Suite, đồng hành cùng các doanh nghiệp tối ưu hệ thống và vận hành an toàn.

PGS.TS Ngô Xuân Bách

Giám đốc Khối Sản phẩm AI, FPT Smart Cloud
Giám đốc Viện Nghiên cứu Quantum AI & Cyber Security, Tập đoàn FPT

2

AI-native Development Platforms

AI-native Development Platforms là gì?

AI-native Development Platforms là thế hệ nền tảng phát triển phần mềm mới, với AI là thành phần cốt lõi, tham gia trực tiếp vào toàn bộ vòng đời phát triển, từ khâu thiết kế, lập trình, kiểm thử, đến rà soát lỗi, viết tài liệu và vận hành hệ thống.

AI giúp tự động hóa các tác vụ lặp lại, cho phép kỹ sư tập trung vào tư duy kiến trúc và giải quyết các bài toán nghiệp vụ phức tạp.

Tiềm năng phát triển

AI-native Development Platforms rút ngắn chu kỳ ra mắt tính năng, chuẩn hoá chất lượng và kiểm soát rủi ro khi tích hợp AI vào quy trình phát triển phần mềm.

Các doanh nghiệp tại Việt Nam sẽ dần chuyển dịch sang mô hình AI-native bởi 4 lý do cấp thiết:

- Năng lực cạnh tranh số buộc các doanh nghiệp tăng tốc đổi tính năng trong thời gian ngắn.
- Cơ sở hạ tầng internet, 5G phổ cập, dịch vụ số bùng nổ kéo theo áp lực mở rộng hệ thống và tốc độ phát triển phần mềm.
- Chuẩn hóa quy trình phát triển từ thiết kế, kiểm thử, triển khai để chạy nhanh mà hạn chế rủi ro.
- Quản trị tập trung bằng cách định danh, phân quyền, kiểm soát dữ liệu và lưu vết, bảo đảm an toàn và tuân thủ.

Ứng dụng thực tế



Ngân hàng – Bảo hiểm

Tự động sinh kiểm thử, rà quét lỗ hổng bảo mật, rút ngắn chu kỳ ra mắt tính năng.



Sản xuất & Logistics

Phát triển các ứng dụng quản lý kho, bảo trì, giám sát vận hành.



Bán lẻ – Thương mại điện tử

Phát triển hệ thống khuyến mãi/ biến động giá; hỗ trợ vận hành, cảnh báo sự cố.



Hành chính công

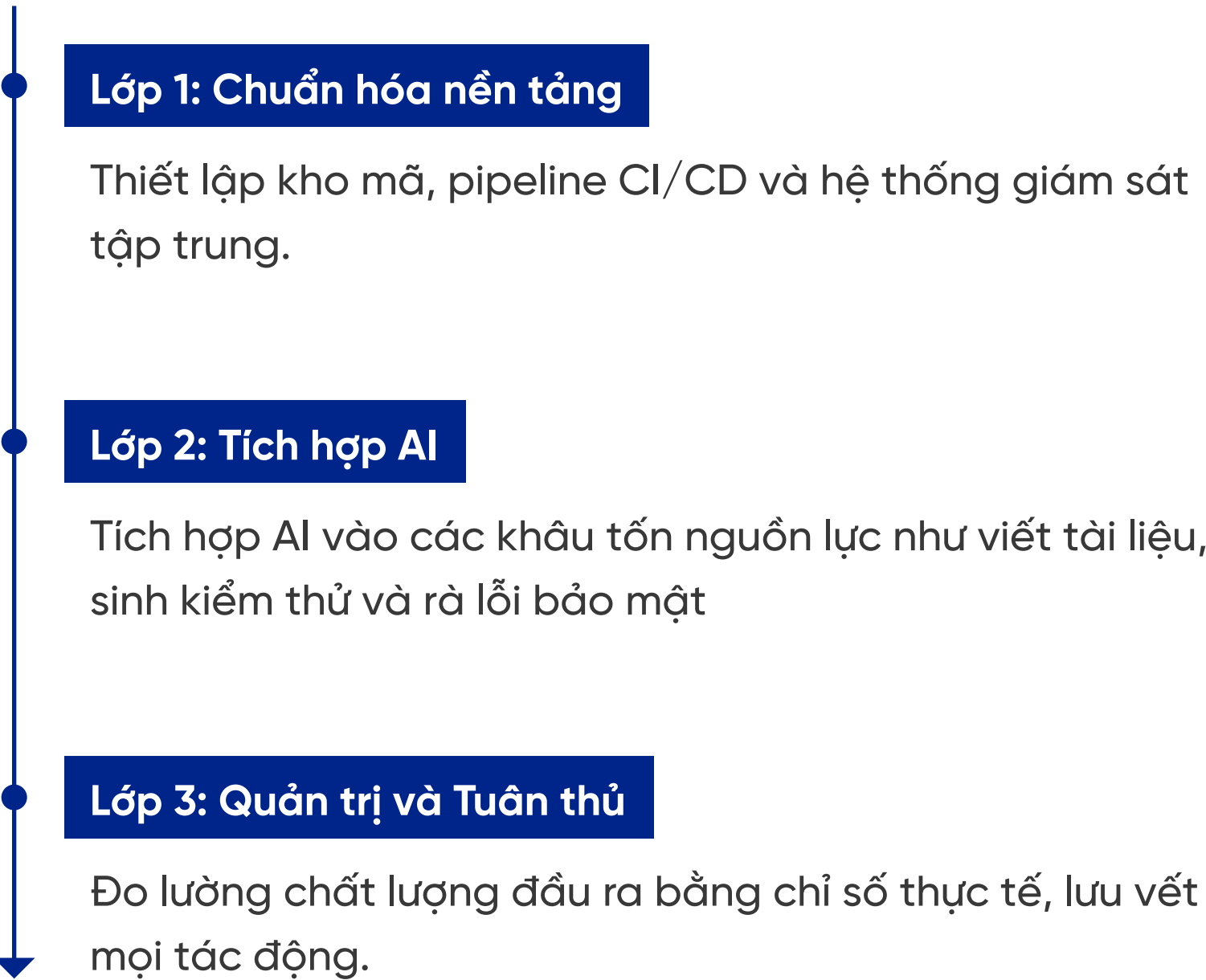
Chuẩn hóa tài liệu, nhật ký vận hành, kiểm thử tự động cổng dịch vụ công.

Góc nhìn doanh nghiệp

Với mục tiêu giúp doanh nghiệp tăng tốc nhưng vẫn kiểm soát hệ thống vận hành một cách hiệu quả, chúng tôi xây dựng và phát triển nền tảng AI thế hệ mới, đồng thời cung cấp một hệ sinh thái hạ tầng đám mây tích hợp bảo mật và quản trị:

- **Môi trường biệt lập:** Đảm bảo mã nguồn doanh nghiệp được huấn luyện và gởi ý trong vùng an toàn (Private/Hybrid Cloud).
- **IDP (Internal Developer Platform):** Xây dựng nền tảng nội bộ chuẩn hóa, giúp kỹ sư tiếp cận các tài nguyên AI một cách chính thống và an toàn.

Mô hình triển khai chuyên nghiệp từ FPT.AI:

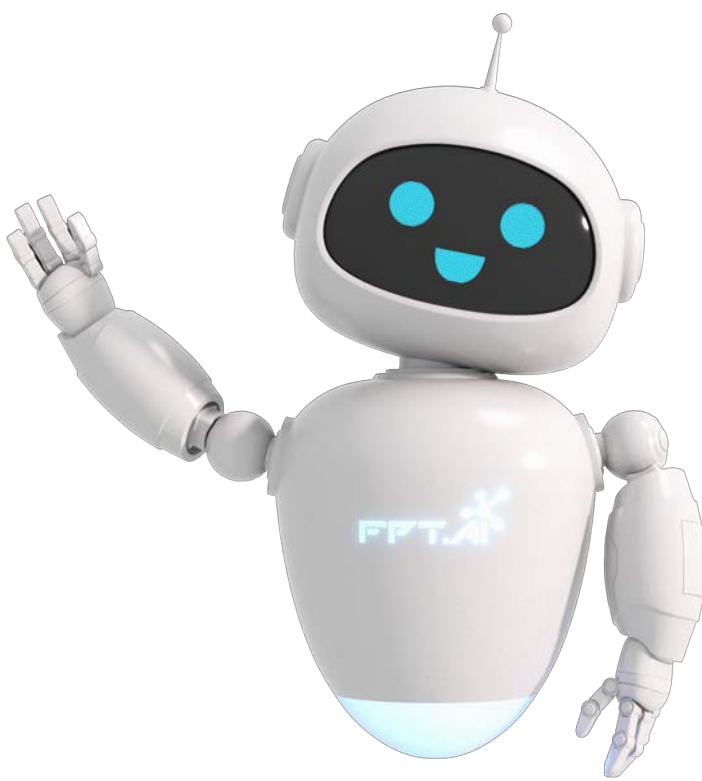


Khuyến nghị trước khi triển khai

- ✓ **Bảo vệ mã nguồn:** Ngăn chặn rò rỉ dữ liệu nhạy cảm bằng cách thiết lập môi trường AI riêng biệt, tránh đưa mã nguồn nội bộ lên các mô hình công cộng.
- ✓ **Tiêu chuẩn kiểm soát:** Mã do AI sinh ra cần được kiểm soát logic chặt chẽ. AI có thể chạy được nhưng dễ mắc sai lầm nếu thiếu tiêu chuẩn rà soát.
- ✓ **An ninh chuỗi cung ứng:** Cảnh giác với các thư viện phụ thuộc chứa mã độc có thể được AI vô tình gợi ý.
- ✓ **Truy vết (Audit Trail):** Phải lưu vết mọi quyết định của AI để phục vụ điều tra sự cố và kiểm toán phần mềm.

Thông điệp

Với hệ sinh thái sản phẩm giải pháp của FPT, chúng tôi kết hợp Hạ tầng Cloud, Dịch vụ triển khai chuyên sâu và Quy trình vận hành chuẩn doanh nghiệp, giúp khách hàng nhanh chóng vận hành thực tế.



3

AI Factory – Computing Infrastructure for AI

AI Factory là gì?

AI Factory là mô hình hạ tầng điện toán đám mây chuyên biệt cho AI, lấy GPU thế hệ mới làm lõi tính toán, kết hợp lưu trữ và phần mềm phát triển, vận hành AI theo một vòng đời khép kín: Từ huấn luyện, tinh chỉnh (fine-tuning), triển khai đến vận hành suy luận (inference) ở quy mô lớn. AI Factory được xem là “chuẩn hạ tầng mới” của kỷ nguyên AI.

Tiềm năng phát triển

- **Nhu cầu xử lý dữ liệu và mô hình tăng theo quy mô số hoá:** Khi doanh nghiệp đẩy mạnh số hoá và tự động hoá, nhu cầu tài nguyên tính toán AI tăng nhanh, đòi hỏi kiến trúc “nhà máy AI” để vận hành tập trung, tránh triển khai rời rạc theo từng dự án.
- **AI có chủ quyền (AI Sovereignty) và sự dịch chuyển hạ tầng (Geopatriation):** Là xu hướng chuyển tải xử lý từ đám mây toàn cầu sang hạ tầng theo vùng/quốc gia để giảm rủi ro địa chính trị và tăng kiểm soát dữ liệu. Do đó, AI Factory trên hạ tầng Cloud nội địa, có chủ quyền là lựa chọn phù hợp cho dữ liệu nhạy cảm.
- **Kỷ luật chi phí AI:** Chi phí GPU và vận hành mô hình dần được quản trị theo vận hành tài chính (FinOps), đo lường theo từng tác vụ, từng phòng ban và gắn với hiệu quả kinh doanh.
- **Hiệu quả năng lượng:** Áp lực điện năng và vận hành trung tâm dữ liệu tăng khiến doanh nghiệp ưu tiên kiến trúc đám mây lai (Hybrid Cloud), tối ưu mật độ tính toán và giảm lãng phí tài nguyên.

Ứng dụng thực tế

Hạ tầng quốc gia (Sovereign AI)

Giúp chính phủ xây dựng năng lực AI nội địa, phát triển mô hình theo dữ liệu và ngôn ngữ địa phương, thúc đẩy kinh tế và nâng cao vị thế quốc gia trong lĩnh vực AI.

Khám phá thuốc & y học cá nhân hóa

Phân tích dữ liệu lớn và ứng dụng Generative AI để phát hiện phân tử thuốc mới, xây dựng phác đồ điều trị cá nhân hóa, nâng cao hiệu quả điều trị và giảm chi phí.

Robot tiên tiến & xe tự hành

Cung cấp năng lực tính toán hiệu năng cao và xử lý dữ liệu thời gian thực để huấn luyện AI, hỗ trợ tự động hóa sản xuất và tăng độ an toàn, chính xác của hệ thống tự hành.

Dịch vụ tài chính an toàn & thông minh

Hỗ trợ phát hiện gian lận giao dịch, tối ưu chăm sóc khách hàng ngân hàng và triển khai giao dịch thuật toán nhờ hạ tầng AI mạnh mẽ, toàn diện.

Góc nhìn doanh nghiệp

Tại Việt Nam, FPT Smart Cloud, thuộc tập đoàn FPT, là đơn vị đầu tiên và duy nhất tại Việt Nam triển khai AI Factory một cách bài bản, phối hợp với hệ sinh thái đối tác quốc tế uy tín như NVIDIA.



Giữ vị trí trung tâm bản đồ công nghệ Việt Nam, FPT định hướng triển khai AI Factory theo mô hình nền tảng, hỗ trợ mục tiêu xây dựng AI có chủ quyền (AI Sovereignty) và đáp ứng xu hướng dịch chuyển tài xử lý về hạ tầng nội địa (Geopatiation):

-  **Tài nguyên tính toán linh hoạt:** GPU Cloud/cụm GPU cho cả huấn luyện và suy luận, hỗ trợ cơ chế đa thuê (multi-tenant) để tối ưu hiệu suất sử dụng.
-  **Vận hành mô hình chuẩn hoá:** Thiết lập tích hợp liên tục/triển khai liên tục (CI/CD) cho mô hình, kho lưu mô hình (model registry), giám sát và truy vết tự động.
-  **Quản trị chi phí AI (FinOps):** Đo chi phí theo thời gian thực, theo tác vụ/đơn vị sử dụng; giúp doanh nghiệp chứng minh tỷ suất hoàn vốn (ROI) minh bạch.

Khuyến nghị trước khi triển khai

- ☒ **Rủi ro chi phí:** GPU nhàn rỗi hoặc phân bổ không tối ưu sẽ trở thành "hố đen" đốt ngân sách. Doanh nghiệp cần cơ chế điều phối tài nguyên thông minh.
- ☒ **Quản trị dữ liệu (Data Governance):** Dữ liệu thiếu chuẩn hóa sẽ tạo ra những dữ liệu "rác", do đó cần lớp lọc dữ liệu sạch trước khi đưa vào nhà máy.
- ☒ **An ninh Zero Trust:** Mô hình và dữ liệu huấn luyện là tài sản quan trọng của doanh nghiệp, cần bảo vệ bằng quản trị danh tính (IAM) và truy vết (Audit trail) nghiêm ngặt.

Thông điệp

Hãy tận dụng AI Factory như một nền tảng chiến lược để tăng tốc phát triển, triển khai và mở rộng AI một cách linh hoạt và đảm bảo tuân thủ trong dài hạn.



4

Domain-specific Language Models (Vertical LLMs)

Domain-specific Language Models là gì?

Domain-specific Language Models (DSLMS), hay **Vertical LLMs**, là các mô hình ngôn ngữ được huấn luyện chuyên sâu cho từng lĩnh vực nghiệp vụ cụ thể như Tài chính, Y tế, Pháp lý hay Sản xuất...

Khác với các mô hình phổ quát (General LLMs) như ChatGPT vốn là "người biết tuốt" nhưng câu trả lời thường chung chung, DSLMs được huấn luyện trên dữ liệu đặc thù, thuật ngữ chuyên môn và quy trình nghiệp vụ riêng biệt. Điều này giúp AI hiểu đúng ngữ cảnh, giảm thiểu hiện tượng "ảo giác" (hallucination) và đưa ra các khuyến nghị có tính tuân thủ cao.

Tiềm năng phát triển

Năm 2026 các doanh nghiệp Việt chuyển trọng tâm sang "GenAI có trách nhiệm". Khi AI tham gia vào nhiều tác vụ ra quyết định rủi ro cao, DSLMs trở thành xu thế bởi 3 giá trị cốt lõi:

- **Độ chính xác và Tin cậy:** AI hiểu rõ các thuật ngữ viết tắt, ký hiệu kỹ thuật và quy định pháp lý đặc thù (ví dụ: Bộ luật Dân sự Việt Nam), đảm bảo đầu ra chính xác hơn mô hình chung.
- **Bảo mật và Quyền riêng tư:** Các doanh nghiệp thường huấn luyện DSLMs trên hạ tầng riêng (Private Cloud) để đảm bảo bí mật kinh doanh không bị rò rỉ ra môi trường công cộng.
- **Tối ưu chi phí & Hiệu năng:** Các mô hình chuyên biệt thường nhỏ gọn hơn (Small Language Models - SLMs) nhưng hiệu quả vượt trội trong lĩnh vực hẹp, giúp giảm chi phí hạ tầng và tăng tốc độ phản hồi.

Ứng dụng thực tế

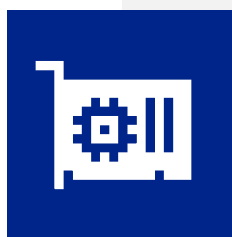
DSLMS đặc biệt phù hợp với nhiều ngành đòi hỏi ngôn ngữ và quy trình đặc thù, đồng thời chịu ràng buộc tuân thủ và độ chính xác cực kỳ cao.



Góc nhìn doanh nghiệp

Hiểu rằng mỗi ngành có ngôn ngữ, quy trình và chuẩn tuân thủ khác nhau, **FPT** định hướng phát triển mô hình ngôn ngữ chuyên ngành như một “lõi năng lực” để doanh nghiệp **khai thác tri thức nội bộ thành lợi thế cạnh tranh**, thay vì chỉ dùng mô hình tổng quát cho mọi bài toán. Trên nền tảng đó, FPT.AI đã phát triển **hơn 50 mô hình ngôn ngữ** phục vụ đa dạng lĩnh vực, giúp doanh nghiệp tăng độ chính xác theo ngữ cảnh ngành, rút ngắn thời gian triển khai và kiểm soát rủi ro tốt hơn khi đưa AI vào vận hành diện rộng.

Để MAS vận hành trong môi trường dữ liệu nhạy cảm, chúng tôi tập trung vào **3 năng lực xuyên suốt**:



Hạ tầng GPU Cloud (FPT AI Factory)

Bảo đảm tài nguyên tính toán đủ mạnh và ổn định để huấn luyện, tinh chỉnh và triển khai mô hình ở quy mô doanh nghiệp.



Vòng quay chất lượng agent (Agent Quality Flywheel)

Tự động hoá chu trình dữ liệu → huấn luyện → đánh giá → triển khai → cải tiến liên tục, giúp mô hình ngày càng phù hợp nghiệp vụ và giảm sai lệch theo thời gian.



Tri thức ngành

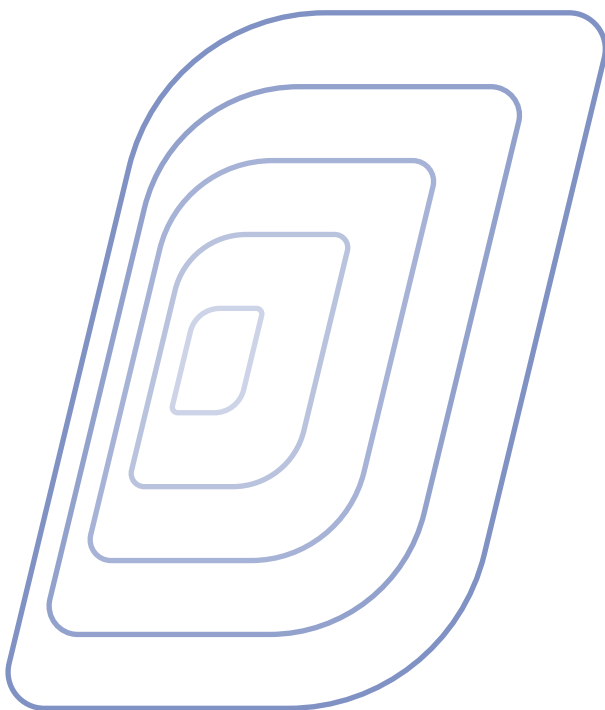
Xây dựng cơ sở tri thức (Knowledge Base) và hệ thống thuật ngữ chuẩn (taxonomy) theo từng ngành, để mô hình “hiểu đúng ngôn ngữ doanh nghiệp” và trả lời nhất quán, có kiểm soát.

Khuyến nghị trước khi triển khai

- ☑ **Nguyên tắc "Garbage in, Garbage out":** Nếu dữ liệu ngành không sạch, AI sẽ học sai. Doanh nghiệp cần chuẩn hóa tri thức nội bộ trước khi huấn luyện.
- ☑ **Cơ chế trích dẫn nguồn:** Nên kết hợp kiến trúc RAG (Retrieval-Augmented Generation) để AI luôn trích dẫn nguồn tài liệu nội bộ, giúp con người dễ dàng kiểm chứng.
- ☑ **Giám sát sự sai lệch (Bias):** Mô hình có thể học theo các thiên kiến từ dữ liệu quá khứ, cần đánh giá định kỳ và thiết lập bộ kiểm thử theo tiêu chuẩn ngành.
- ☑ **Chi phí vận hành dài hạn:** Việc tinh chỉnh và cập nhật DSLMs tốn kém nguồn lực; doanh nghiệp nên bắt đầu bằng các bài toán có ROI rõ ràng trước khi mở rộng.

Thông điệp

Trong kỷ nguyên AI, lợi thế cạnh tranh không nằm ở việc sở hữu công nghệ, mà nằm ở việc sở hữu mô hình AI hiểu sâu sắc tri thức và dữ liệu của chính doanh nghiệp bạn.



5

AI Governance & AI Security Platforms

AI Governance & AI Security Platforms là gì?

Để AI đi vào vận hành thực tế, doanh nghiệp cần kết hợp **Quản trị AI (AI Governance)** và **Nền tảng bảo mật AI (AI Security Platforms)** theo cách bổ trợ lẫn nhau:

- **Quản trị AI (AI Governance):** Bộ nguyên tắc và cơ chế quản trị vòng đời AI (từ Dữ liệu – Mô hình – Agent), để xác định dữ liệu được phép dùng, quyền truy cập theo vai trò, yêu cầu kiểm soát sai lệch (bias), ảo giác (hallucination), và lưu vết (audit trail) để chứng minh tuân thủ.
- **Nền tảng bảo mật AI (AI Security Platforms):** Hệ thống bảo vệ trước các rủi ro an ninh khi triển khai AI, gồm tấn công tiêm lệnh (prompt injection), rò rỉ dữ liệu qua nhật ký hệ thống, lạm quyền của AI agents và rủi ro từ chuỗi cung ứng mô hình.

Tiềm năng phát triển

Năm 2026 là điểm bùng phát nhu cầu quản trị AI khi rủi ro chuyển dịch từ "trả lời sai" sang "hành động sai":

- **Cú hích pháp lý: Luật Bảo vệ dữ liệu cá nhân** đặt ra yêu cầu mới về quản trị dữ liệu nhạy cảm. AI Security/Governance lúc này trở thành "hạ tầng tuân thủ" bắt buộc.
- **Thực trạng an ninh mạng:** Với hơn **552.000 cuộc tấn công mạng⁽¹⁰⁾** ghi nhận tại Việt Nam năm 2025, AI vô tình làm tăng bề mặt tấn công. Doanh nghiệp cần một cơ chế giám sát liên tục thay vì đánh giá theo đợt.
- **Áp lực chuẩn hóa toàn cầu:** Các tiêu chuẩn như **EU AI Act** yêu cầu quản trị rủi ro cao, buộc doanh nghiệp Việt phải chuẩn bị cơ chế kiểm soát tương đương khi làm việc với thị trường/đối tác EU.

Ứng dụng thực tế



Tài chính – Ngân hàng

Kiểm soát rủi ro mô hình tín dụng, lưu vết mọi quyết định của AI để giải trình và chống gian lận tài chính.



Y tế

Thiết lập hàng rào bảo vệ dữ liệu, kiểm soát quyền truy cập hồ sơ bệnh án theo vai trò (RBAC) và audit nghiêm ngặt.



Bán lẻ – Thương mại điện tử

Ngăn chặn AI "bịa" chính sách hoặc rò rỉ lịch sử mua sắm của khách hàng.



Hành chính công

Chống hiện tượng "bịa" quy định, đảm bảo chính xác nguồn tri thức, có kiểm chứng.

Góc nhìn doanh nghiệp

Ở cấp độ doanh nghiệp, rủi ro nằm ở quyền truy cập, hành động và trách nhiệm pháp lý. Vì vậy, triển khai AI ở cấp độ doanh nghiệp cần quản trị và bảo mật ngay từ bước đầu tiên.

Chúng tôi khuyến nghị triển khai theo khung 5 lớp:

- 1 **Phân loại dữ liệu:** Xác định dữ liệu nhạy cảm và phạm vi được phép dùng cho AI.
- 2 **Phân loại rủi ro:** Đánh giá mức độ tác động của từng trường hợp cụ thể.
- 3 **Quản trị danh tính (IAM):** Kiểm soát tuyệt đối quyền truy cập của người dùng và Agent.
- 4 **Giám sát thời gian chạy:** Theo dõi truy cập, hành động, chất lượng đầu ra và hiện tượng trôi mô hình (drift model) theo thời gian thực.
- 5 **Phòng thủ chủ động:** Chặn đứng các cuộc tấn công chèn lệnh (Prompt Injection) và ngăn rò rỉ dữ liệu.



Về triển khai thực tế, chúng tôi tập trung **3 năng lực cốt lõi**, giúp doanh nghiệp mở rộng AI nhanh nhưng vẫn kiểm soát được dữ liệu, hành vi của AI Agent và rủi ro pháp lý.

Dấu vết kiểm toán (audit trail)	Kiểm thử tấn công (red teaming)	Nền tảng cloud nội địa
Truy vết và đáp ứng tuân thủ.	Trước khi vận hành chính thức (go-live).	Hỗ trợ chủ quyền dữ liệu và giảm rủi ro phụ thuộc hạ tầng xuyên biên giới.

Khuyến nghị trước khi triển khai

- ✓ **Tránh quản trị hình thức:** Có chính sách nhưng không có công cụ giám sát (logging/audit) để theo dõi, truy vết thì không kiểm soát được rủi ro thực tế.
- ✓ **Cân bằng giữa Kiểm soát và Đổi mới:** Nếu siết quá chặt, nhân viên sẽ tìm đến "Shadow AI" (công cụ ngoài). Cần phân tầng rủi ro để áp dụng mức độ kiểm soát phù hợp.
- ✓ **Chống lạm quyền Agent:** Mỗi AI Agent phải được định danh và giới hạn quyền hành động như một nhân sự thật.
- ✓ **Cơ chế Human-in-the-loop:** Thiết lập các điểm phê duyệt của con người cho những hành động nhạy cảm (chuyển tiền, xóa dữ liệu...).

Thông điệp

Không đợi đến khi sự cố xảy ra mới tìm cách bảo mật, một hệ thống AI không có quản trị giống như chiếc xe đua không phanh: tốc độ càng cao, nguy hiểm càng lớn. FPT cung cấp "hệ thống phanh" an toàn để doanh nghiệp tự tin bứt phá.



6 Preemptive Cybersecurity

Preemptive Cybersecurity là gì?

Preemptive Cybersecurity (An ninh mạng tiền phát) là cách tiếp cận chủ động, dựa trên tự động hóa để liên tục kiểm thử, dự báo và ngăn chặn các mối đe dọa trước khi chúng kịp gây hại. Thay vì đợi sự cố xảy ra rồi mới phản ứng, mô hình này đưa hoạt động **Tấn công mô phỏng (Offensive Testing)** vào chu trình vận hành hàng ngày.

Trọng tâm của xu hướng này gồm 3 lớp năng lực:

- **Phát hiện sớm:** Giám sát liên tục để nhận ra dấu hiệu bất thường từ rất nhỏ.
- **Ưu tiên đúng:** Chấm điểm rủi ro để tập trung vào lỗ hổng có khả năng gây thiệt hại lớn.
- **Tự động xử lý:** Cô lập, chặn hoặc khôi phục theo kịch bản đã kiểm soát.

Tiềm năng phát triển

Năm 2026, Preemptive Cybersecurity sẽ trở thành nhu cầu cấp thiết tại Việt Nam bởi:

- **Sự cố thực tế gia tăng: 552.000 cuộc tấn công mạng** tại Việt Nam với 52,3% tổ chức đã từng bị xâm nhập ít nhất một lần. Cách làm “đánh giá theo đợt” không còn theo kịp bề mặt tấn công mở rộng.
- **Thiếu nhân lực:** Gần **48%** doanh nghiệp, tổ chức⁽¹⁰⁾ thiếu nhân sự an ninh mạng chuyên trách buộc doanh nghiệp phải **tự động hoá** nhiều khâu phát hiện, ngăn chặn để duy trì mức bảo vệ.
- **Sự bùng nổ của AI Agents:** Khi AI Agents tham gia vào vận hành, cần định danh, phân quyền, bảo vệ như một danh tính rủi ro trong hệ thống.

Ứng dụng thực tế



Tài chính – Ngân hàng

Tự động phát hiện và phản ứng sự cố; chặn truy cập bất thường; bảo vệ định danh số và giao dịch theo thời gian thực.



Sản xuất – Logistics

Giám sát rủi ro từ thiết bị IoT/OT, phát hiện sớm dấu hiệu mã độc xâm nhập, tránh gây đứt gãy chuỗi vận hành.



Bán lẻ – Thương mại điện tử

Chặn agents càn quét dữ liệu, ngăn rò rỉ thông tin khách hàng và giám sát các hành vi gian lận khuyến mãi tinh vi.



Hành chính công

Bảo vệ dữ liệu nhạy cảm của người dân; cảnh báo sớm xâm nhập và lưu vết đầy đủ phục vụ công tác điều tra.

Góc nhìn doanh nghiệp

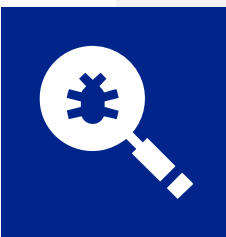
Tại FPT, FPT Smart Cloud củng cố năng lực bảo mật bằng cách tích hợp Preemptive Cybersecurity vào nền tảng FPT Cloud và FPT.AI, giúp doanh nghiệp nghiệp phát hiện sớm sự cố.

Chúng tôi tư vấn triển khai bảo mật chủ động dựa trên **3 trụ cột nền tảng**:



Dự báo từ mối đe dọa (Threat Intelligence)

AI liên tục quét dữ liệu để nhận diện dấu hiệu tấn công mới, cập nhật cảnh báo và quy tắc phòng thủ.



Săn tìm mối đe dọa tự động (Autonomous Threat Hunting)

Các AI Agent bảo mật thực hiện kiểm thử và mô phỏng tấn công trong phạm vi được cấp quyền, phát hiện điểm yếu, đề xuất biện pháp khắc phục và tự động vá lỗi.



Phân tích hành vi (Behavioral Analytics)

Khi có dữ liệu đột ngột truy cập bất thường, hệ thống sẽ tự động cô lập thực thể đó ngay lập tức để ngăn chặn thiệt hại lan rộng.

Chúng tôi tích hợp năng lực an ninh mạng vào nền tảng FPT Cloud, giúp doanh nghiệp tự động hoá ứng cứu, triển khai bảo mật ngay từ khâu thiết kế và chặn sớm tấn công trước khi lan rộng.

Khuyến nghị trước khi triển khai

- ☑ **Ngưỡng tin cậy:** Tự động phản ứng phải đi kèm cơ chế phê duyệt cho các hành động nhạy cảm để tránh gây gián đoạn hoạt động ngoài ý muốn.
- ☑ **Giảm "Nhiều" cảnh báo:** Tránh tình trạng quá tải (Alert Fatigue) bằng cách ưu tiên các lỗ hổng có ảnh hưởng trực tiếp đến logic nghiệp vụ.
- ☑ **Bảo vệ quyền riêng tư:** Giám sát sâu phải song hành với phân loại dữ liệu và nguyên tắc "Quyền truy cập tối thiểu" (Least Privilege).

Thông điệp

Trong kỷ nguyên AI, bảo mật phải đi trước rủi ro. FPT giúp doanh nghiệp phát hiện sớm - ngăn chặn sớm - ứng cứu tự động, để triển khai AI an toàn và đúng tuân thủ.



7

Computer Vision & Vision Agents

Computer Vision & Vision Agents là gì?

Năm 2026, **Computer Vision (Thị giác máy tính)** không chỉ dừng ở việc “nhìn và nhận dạng”, mà phát triển thành các **Vision Agents**: Hệ thống có khả năng quan sát, suy luận theo ngữ cảnh và thực thi các tác vụ theo quy trình nghiệp vụ.

- **Computer Vision** là lớp năng lực xử lý ảnh/video để trích xuất thông tin có cấu trúc (đối tượng, lỗi, hành vi, văn bản trong ảnh...).
- **Vision Agents** là “nhân sự AI” hoàn chỉnh. Vision Agents kết hợp **Computer Vision** với các **Mô hình Ngôn ngữ thị giác (Vision-Language Models)** để máy không chỉ “thấy” mà còn “hiểu” bối cảnh. Vision Agents có thể tự lập kế hoạch, gọi API kết nối với các hệ thống khác và ra quyết định thực thi theo mục tiêu nghiệp vụ.

Trong hệ thống MAS, Vision Agents đóng vai trò là “người trinh sát”, chịu trách nhiệm Quan sát thực tế, biến hình ảnh thành thông tin số và kích hoạt các chuỗi hành động liên hoàn cho các agent khác.

Tiềm năng phát triển

Thị trường Việt Nam đang hội tụ 3 yếu tố thúc đẩy Vision Agents tăng tốc:

- **Nhu cầu tự động hóa tăng mạnh:** Doanh nghiệp muốn tăng năng suất nhưng không thể phụ thuộc hoàn toàn vào Cloud, do độ trễ và tính sẵn sàng của kết nối.
- **Phát triển Đô thị thông minh:** Hà Nội và TP.HCM đã tiên phong vận hành hàng nghìn Camera AI. Ví dụ, Hà Nội đã phát hiện hơn **6.300 trường hợp vi phạm giao thông⁽¹⁾** qua “phạt nguội” bằng Camera AI. Đây là minh chứng rõ nét cho hiệu quả vận hành thực tế.
- **Sự trưởng thành của Edge AI:** Xử lý hình ảnh ngay trên camera/thiết bị giúp giảm độ trễ, giảm tải truyền dữ liệu và giữ dữ liệu nhạy cảm tại chỗ.

Ứng dụng thực tế

Vision Agents được triển khai vào 4 nhóm giải pháp mũi nhọn:



Sản xuất – Kho bãi

Kiểm tra lỗi ngoại quan; giám sát an toàn lao động để cảnh báo/ứng cứu kịp thời...



Bán lẻ & Trải nghiệm khách hàng

Nhận diện kệ hàng trống; phân tích bản đồ nhiệt để tối ưu bố trí và luồng di chuyển...



Dịch vụ công & Tài chính

Định danh điện tử (eKYC), chống deep-fake; bóc tách dữ liệu hóa đơn/chứng từ...



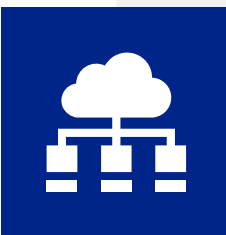
Y tế & Chăm sóc sức khỏe

Theo dõi người bệnh, đưa ra cảnh báo, giúp giảm tải giám sát cho đội ngũ y bác sĩ...

Góc nhìn doanh nghiệp

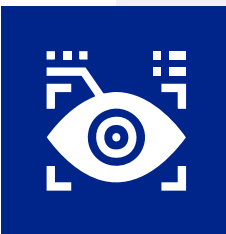
Tại FPT, tiếp cận Vision Agents như một bài toán triển khai vận hành, dựa trên

3 năng lực triển khai cốt lõi:



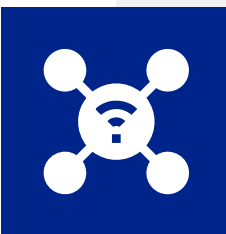
Hạ tầng triển khai linh hoạt

Chạy được cả trên cả Nền tảng Cloud và Trí tuệ nhân tạo tại biên (edge AI) để xử lý hình ảnh thời gian thực, giảm độ trễ và tối ưu chi phí.



Giải pháp thị giác đã kiểm chứng

Kế thừa các năng lực như eKYC, OCR và các mô-đun phân tích hình ảnh đã triển khai ở nhiều doanh nghiệp lớn.



Tích hợp vào quy trình vận hành

Kết nối camera/IoT với hệ thống nghiệp vụ (cảnh báo, xử lý, báo cáo...), kèm phân quyền và ghi vết để quản trị rủi ro.



Khuyến nghị trước khi triển khai

- ☑ **Ưu tiên quyền riêng tư:** Chỉ thu thập hình ảnh khi có mục đích rõ ràng; phân quyền truy cập chặt; ghi nhật ký truy cập và thao tác (audit trail) đầy đủ.
- ☑ **Kiểm soát sai số theo bối cảnh:** Ánh sáng, góc quay, che khuất có thể gây cảnh báo sai. Cần chuẩn hoá thiết bị đầu vào và kiểm định mô hình định kỳ.
- ☑ **Tối ưu chi phí lưu trữ:** Video là dữ liệu rất nặng. Nên xử lý tại biên (edge) và chỉ đẩy lên Cloud phần dữ liệu cần thiết để giảm tải mạng và chi phí.

Thông điệp

Dữ liệu năm 2026 xuất hiện ở mọi nơi thông qua ống kính Camera. Doanh nghiệp nào 'nhìn thấy' và xử lý hình ảnh nhanh nhất, doanh nghiệp đó sẽ làm chủ cuộc chơi vận hành thực địa.



8

Physical AI

Physical AI là gì?

Physical AI (AI vật lý) là các hệ thống trí tuệ nhân tạo có khả năng nhận biết, suy luận, ra quyết định và thực thi hành động trực tiếp trong môi trường vật lý. Physical AI thường kết hợp robot, cảm biến, hệ thống tự động hoá, và bản sao số (digital twin) để mô phỏng, giám sát và tối ưu vận hành ngoài đời thực.

Khác với AI tạo sinh (generative AI) chủ yếu xử lý dữ liệu số như văn bản, hình ảnh, âm thanh, Physical AI tập trung vào chu trình khép kín: **Nhận biết (cảm biến) → Suy luận (AI) → Quyết định → Hành động (cơ cấu chấp hành).**

Tiềm năng phát triển

Năm 2025, **tổng kim ngạch xuất khẩu** của Việt Nam đạt khoảng **475 tỷ USD⁽¹²⁾** và FDI giải ngân liên tục tăng trưởng. Việt Nam có nền tảng thuận lợi để triển khai **AI vật lý (Physical AI)** nhờ quy mô sản xuất gắn với xuất khẩu rất lớn và dòng vốn đầu tư tiếp tục duy trì ở mức cao.

- **Giảm áp lực nhân công và an toàn lao động:** Tự động hoá các công việc nặng nhọc, độc hại, đòi hỏi lặp lại chính xác như bốc xếp, kiểm tra, vận chuyển trong nhà máy.
- **Tăng sức cạnh tranh sản xuất xuất khẩu:** Nâng tỷ lệ đạt chuẩn, giảm thời gian dừng máy, tối ưu vận hành dây chuyền.
- **Dữ liệu hiện trường ngày càng sẵn:** Mạng lưới cảm biến, thiết bị quan sát và hệ thống vận hành số, tạo đầu vào để AI ra quyết định và điều khiển theo thời gian thực.

Ứng dụng thực tế

Physical AI đang tạo khác biệt rõ ở các ngành trọng điểm tại Việt Nam:



Sản xuất thông minh

Robot cộng tác (cobot) hỗ trợ lắp ráp, kiểm tra, bốc xếp; tự điều chỉnh thao tác khi thay đổi linh kiện hoặc khi dây chuyền có bất thường.



Nông nghiệp công nghệ cao

Robot/cảm biến nhận diện độ chín, phát hiện vùng cây bệnh để phun/thu hoạch theo điểm, giảm lãng phí vật tư và công lao động.



Logistics & Kho bãi

Xe tự hành (AGV/AMR) tự tối ưu lộ trình trong kho, tránh vật cản và phối hợp theo nhóm để tăng tốc độ xử lý hàng.

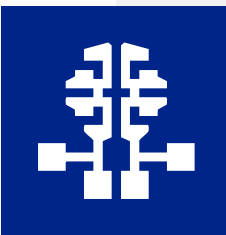


Hạ tầng & Đô thị

Hệ thống giám sát phát hiện sớm sự cố điện, trạm biến áp, nguy cơ cháy nổ hoặc hư hỏng công trình theo thời gian thực để kịp thời xử lý.

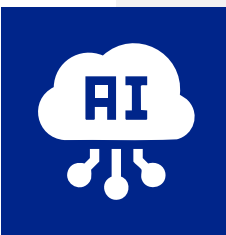
Góc nhìn doanh nghiệp

Trong tương lai, Physical AI có thể trở thành 1 mảnh ghép trong hệ sinh thái "AI-Nation". Bởi Physical AI có tiềm năng tạo ra giá trị cao khi được triển khai theo kiến trúc "từ hiện trường đến trung tâm", vừa đáp ứng thời gian thực, vừa quản trị được dữ liệu, mô hình và tích hợp vào hệ thống vận hành.



Xử lý tại hiện trường (Edge)

Chạy suy luận (inference) ngay tại nhà máy/kho để độ trễ thấp, vận hành ổn định khi kết nối gián đoạn.



Nền tảng Cloud cho huấn luyện & vận hành (AI Factory)

Tập trung dữ liệu lớn để huấn luyện, mô phỏng bằng bản sao số (Digital Twin) và quản trị vòng đời mô hình (MLOps).



Tích hợp công nghiệp

Kết nối AI với hệ thống điều khiển và quản trị như PLC/SCADA, ERP/MES/WMS để AI có thể triển khai vào quy trình thực tế.

Với hạ tầng tính toán GPU, nền tảng quản trị mô hình và năng lực tích hợp hệ thống của FPT Smart Cloud cùng hệ sinh thái công nghệ của FPT, doanh nghiệp có thể triển khai Physical AI theo lộ trình rõ ràng:

**Làm được ở hiện trường → Quản trị được ở trung tâm
→ Mở rộng được theo quy mô vận hành.**

Khuyến nghị trước khi triển khai

- ☑ **Khoảng cách giữa Mô hình và Hiện trường:** Ánh sáng, bụi và rung chấn có thể làm "trôi" mô hình (Model drift). Cần cơ chế giám sát và hiệu chỉnh định kỳ.
- ☑ **Tích hợp IT - OT:** Kết nối giữa hệ thống phần mềm (IT) và hệ thống vận hành máy móc (OT) cần được phân vùng mạng và bảo mật Zero Trust để tránh rủi ro tấn công xuyên suốt.
- ☑ **Cơ chế giới hạn hành vi:** AI điều khiển vật lý bắt buộc phải có "chốt chặn an toàn" (Hard-stop) và kịch bản ứng phó ngoại lệ để bảo vệ con người.
- ☑ **ROI thực dụng:** Nên bắt đầu từ những "điểm đau" cụ thể như giảm lỗi sản phẩm hoặc tối ưu điện năng thay vì triển khai dàn trải toàn nhà máy.

Thông điệp

Nếu Multi-agent Systems (MAS) là hệ điều hành số, thì Physical AI chính là "cánh tay" thực thi. Sự kết hợp này giúp các doanh nghiệp tự động hóa dây chuyền/kho vận, từng bước chuyển dịch từ gia công giá rẻ sang sản xuất thông minh và tự chủ.



9

Digital Provenance & Content Integrity

Digital Provenance & Content Integrity là gì?

Digital Provenance (Nguồn gốc số) và **Content Integrity (Tính toàn vẹn nội dung)** là bộ đôi công nghệ, giúp **xác thực nguồn gốc và trạng thái của nội dung số**: nội dung do ai tạo, tạo khi nào, tạo bằng công cụ nào (AI hay con người) và **có bị sửa đổi sau khi phát hành hay không**.

- **Digital Provenance:** Ghi lại “lý lịch” nội dung theo chuỗi sự kiện (tạo mới, chỉnh sửa, xuất bản), gắn kèm siêu dữ liệu (metadata) và cơ chế xác thực như chữ ký số/hàm băm; có thể kết hợp dấu nước số (watermarking) để nhận diện nội dung do AI tạo hoặc đã qua xử lý.
- **Content Integrity:** Cơ chế phát hiện và cảnh báo thay đổi trái phép. Khi nội dung bị chỉnh sửa không đúng quy trình/không khớp chữ ký số hoặc giá trị băm, hệ thống sẽ ghi nhận và cảnh báo.

Tiềm năng phát triển

Khi Deepfake trở nên khó phân biệt bằng mắt thường, xác thực nguồn gốc và bảo toàn nội dung trở thành nhu cầu cấp thiết tại Việt Nam:

- **Chống lừa đảo và mạo danh:** Năm 2025, Việt Nam thiệt hại khoảng **6.000 tỷ đồng**⁽¹³⁾ do lừa đảo trực tuyến ngày càng tinh vi. Digital Provenance giúp doanh nghiệp xác thực nguồn gốc nội dung trước khi dùng cho eKYC, chăm sóc khách hàng, truyền thông thương hiệu.
- **Tuân thủ pháp lý:** Các quy định mới đặt trọng tâm vào quản trị rủi ro và yêu cầu minh bạch để nhận biết các nội dung do AI tạo ra. Digital Provenance giúp “đóng dấu” và kiểm chứng lịch sử nội dung để đáp ứng tuân thủ.
- **Chuẩn hóa theo tiêu chuẩn quốc tế:** Các khung như **C2PA** đang được nhiều hãng công nghệ và truyền thông thúc đẩy để xác thực nguồn gốc nội dung, giảm rủi ro tin giả/deepfake. Các doanh nghiệp Việt muốn làm việc với đối tác quốc tế sẽ cần tương thích tiêu chuẩn xác thực này để bảo vệ thương hiệu và tài sản số.

Ứng dụng thực tế



Chống giả mạo hợp đồng/biên bản; xác thực nguồn gốc dữ liệu đầu vào cho các mô hình chấm điểm tín dụng.



Gắn nhãn và quản trị nội dung do AI tạo; chứng minh nội dung để bảo vệ thương hiệu.



Xác thực văn bản, thông cáo và nội dung công bố chính thống; giảm rủi ro phát tán thông tin giả mạo gây nhiễu dư luận.

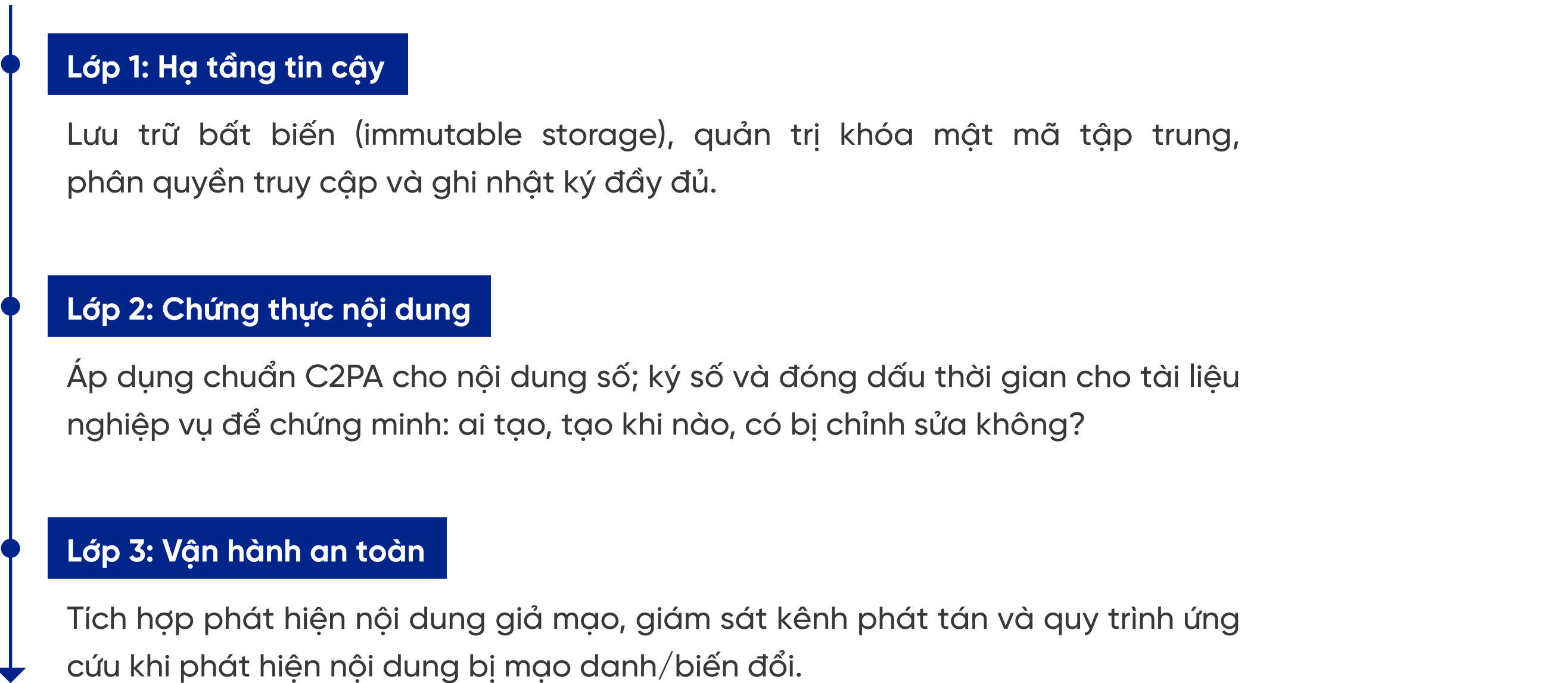


Trong hệ thống hàng nghìn Agent tự động, Digital Provenance giúp xác thực nội dung do agents tạo ra trước khi xử lý.

Góc nhìn doanh nghiệp

Để dùng AI ở quy mô vận hành, doanh nghiệp cần **lớp tin cậy (trust layer)** nhằm **xác thực nguồn gốc, đảm bảo nội dung không bị sửa và truy vết được trách nhiệm**, từ đó giảm rủi ro mạo danh, tin giả và thất thoát dữ liệu.

Chúng tôi khuyến nghị triển khai theo 3 lớp để áp dụng vào thực tế:



Khi tích hợp vào hệ sinh thái FPT, **trust layer** giúp doanh nghiệp:

- **Kiểm soát nguồn gốc dữ liệu và mô hình trong AI Factory:** Quản trị hồ sơ nguồn gốc mô hình (MLBOM – Machine Learning Bill of Materials) để giảm rủi ro chuỗi cung ứng mô hình và dữ liệu bản.
- **Bảo vệ tài sản trí tuệ:** Chứng minh quyền sở hữu nội dung/dữ liệu, hỗ trợ xử lý tranh chấp và hạn chế nguy cơ bị trích xuất dữ liệu để huấn luyện trái phép.

Khuyến nghị trước khi triển khai

- ☑ **Rủi ro mất thông tin nguồn gốc:** Dấu vết trong tệp có thể bị mất khi người dùng chụp màn hình, nén file hoặc đăng lên nền tảng không hỗ trợ. Nên áp dụng kết hợp: Thông tin nguồn gốc trong tệp, ký số/đóng dấu thời gian và quy trình phê duyệt.
- ☑ **Quy định rõ điểm “ký”:** Xác định rõ ký ở dữ liệu đầu vào, dữ liệu huấn luyện, hay đầu ra phát hành, người chịu trách nhiệm ký và tiêu chí ký để phục vụ kiểm toán, đối soát sau này.
- ☑ **Không thay thế an ninh mạng và quản trị rủi ro:** Xác thực nguồn gốc chỉ giúp chứng minh/đối chiếu. Doanh nghiệp vẫn cần lớp chống gian lận, kiểm soát truy cập, giám sát sự cố và quy trình xử lý khủng hoảng truyền thông khi có nội dung giả mạo.

Thông điệp

Trong kỷ nguyên nội dung do AI tạo ra, khả năng xác thực nguồn gốc và đảm bảo tính toàn vẹn dữ liệu/nội dung sẽ trở thành điều kiện nền tảng để vận hành số an toàn và đáng tin cậy.



10 Quantum Computing

Quantum Computing là gì?

Quantum Computing (Điện toán lượng tử) là mô hình tính toán dùng **qubit** (đơn vị thông tin lượng tử) thay cho **bit** 0/1 truyền thống. Nhờ các hiện tượng vật lý như **chồng chập (superposition)** và **rối lượng tử (entanglement)**, hệ thống lượng tử có thể xử lý một số bài toán theo cách khác hẳn máy tính cổ điển, đặc biệt ở các bài toán tối ưu, mô phỏng vật liệu, hóa học và mật mã.

Từ 2026, các hãng công nghệ lớn như IBM và Microsoft sẽ có nhiều bước phát triển vượt trội trong lĩnh vực điện toán lượng tử, từ nghiên cứu sang triển khai có kế hoạch, đặc biệt ở các bài toán mô phỏng và an toàn mật mã.

Tiềm năng phát triển

Điện toán lượng tử tại Việt Nam không còn là lý thuyết xa vời mà đã có những bước đi cụ thể:

- **Chính sách xác định hướng đi:** Việt Nam chính thức đưa Điện toán lượng tử vào nhóm công nghệ chiến lược theo **Quyết định 1131/QĐ-TTg (06/2025)**, tạo hành lang pháp lý và nguồn lực cho giai đoạn 2026–2030.
- **Cộng đồng chuyên gia mở rộng:** Mạng lưới VNQuantum ra mắt 08/2025 với hơn **2.000 thành viên**, kết nối các chuyên gia hàng đầu từ 22 quốc gia, hỗ trợ kết nối nghiên cứu và thử nghiệm ứng dụng.
- **Doanh nghiệp lớn đã đầu tư:** FPT thành lập Viện nghiên cứu **Quantum AI & An ninh mạng (QACI)** với vốn đầu tư **100 triệu USD**, khẳng định vị thế dẫn dắt của FPT trong nghiên cứu và ứng dụng công nghệ này.

Ứng dụng thực tế



Tài chính – Ngân hàng

Tối ưu hóa danh mục đầu tư, quản trị rủi ro biến động và thanh khoản với tốc độ siêu tốc.



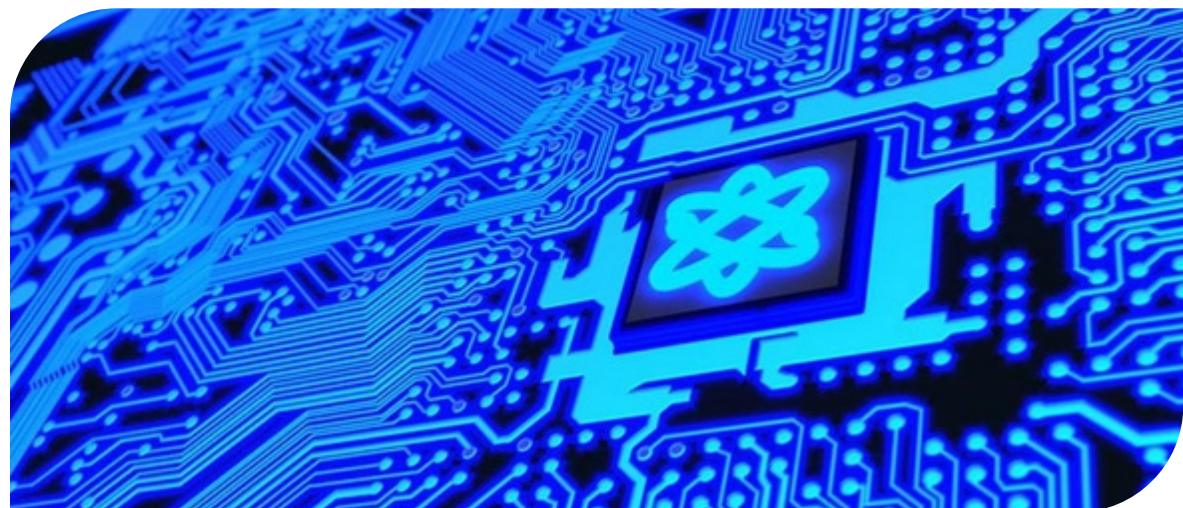
Y dược & Năng lượng

Mô phỏng phân tử/vật liệu để rút ngắn thử nghiệm R&D; tối ưu vận hành lưới điện và cân bằng phụ tải.



Logistics – Sản xuất

Tối ưu lịch sản xuất, phân bổ nguồn lực và tuyến vận tải; điều phối chuỗi cung ứng phức tạp.



Góc nhìn doanh nghiệp

Năm 2026, điện toán lượng tử tại Việt Nam chủ yếu vẫn ở giai đoạn nghiên cứu và thử nghiệm. Các doanh nghiệp nên có sự chuẩn bị sẵn sàng để đón đầu xu hướng khi công nghệ đạt ngưỡng ứng dụng.

3 hướng nghiên cứu và thử nghiệm thực tế:



Chọn đúng bài toán

Ưu tiên nhóm bài toán có lợi thế rõ ràng nếu dùng lượng tử, như tối ưu hoá (lịch sản xuất, tuyến vận tải, phân bổ nguồn lực) và mô phỏng vật liệu/phân tử.



Thiết kế mô hình triển khai hybrid

Dùng hạ tầng tính toán hiệu năng cao để xử lý dữ liệu và chạy mô phỏng; khi phù hợp mới thử nghiệm phần “lõi tối ưu” trên đám mây lượng tử (Quantum Cloud).



Chuẩn bị bảo mật hậu lượng tử

Lập kế hoạch chuyển dần sang mã hoá kháng lượng tử cho các hệ thống cần bảo vệ dài hạn, vì rủi ro trong tương lai có thể xảy ra với dữ liệu lưu trữ từ hôm nay.

Khuyến nghị trước khi triển khai

- ✔ **Không tự đầu tư máy tính lượng tử:** Hạ tầng lượng tử đòi hỏi điều kiện vận hành đặc thù và chi phí rất cao. Doanh nghiệp nên tiếp cận qua dịch vụ đám mây lượng tử hoặc các chương trình thử nghiệm với đối tác.
- ✔ **Chuẩn bị nhân lực và năng lực triển khai:** Nguồn nhân lực lượng tử và kiến trúc sư hệ thống lai (hybrid) khan hiếm. Doanh nghiệp cần kế hoạch đào tạo, tuyển dụng hoặc hợp tác với các viện/trung tâm nghiên cứu.
- ✔ **Rủi ro an toàn thông tin:** Dữ liệu có vòng đời dài (tài chính, y tế) cần được nâng cấp sang Mật mã kháng lượng tử để tránh nguy cơ bị giải mã trong tương lai.

Thông điệp



“
Hãy bắt đầu bằng thử nghiệm nhỏ có mục tiêu, có chỉ số đo hiệu quả, đồng thời xây năng lực nội bộ về dữ liệu, thuật toán và an ninh thông tin để sẵn sàng mở rộng khi thị trường chín.”

PGS.TS Ngô Xuân Bách

Giám đốc Khối Sản phẩm AI, FPT Smart Cloud
Giám đốc Viện Nghiên cứu Quantum AI & Cyber Security, Tập đoàn FPT

Bước tiếp theo cho doanh nghiệp

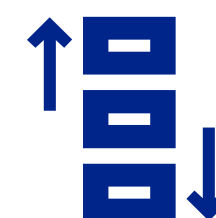
Từ chiến lược đến triển khai: chuẩn hóa dữ liệu, hạ tầng và bảo mật để mở rộng AI an toàn, đo được hiệu quả và tối ưu chi phí dài hạn.



Đánh giá & Chuẩn hóa

Chuẩn hóa nền móng AI

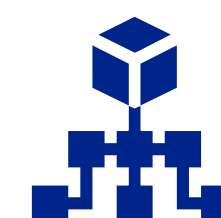
Đánh giá mức sẵn sàng theo 4 trụ cột: dữ liệu - hạ tầng - bảo mật - vận hành, xác định điểm nghẽn và lộ trình khắc phục.



Ưu tiên đúng bài toán

Chọn bài toán tạo tác động nhanh

Ưu tiên các kịch bản có dữ liệu sẵn, quy trình rõ và chỉ số đo lường cụ thể để tạo kết quả trong ngắn hạn, làm nền cho mở rộng.



Kiến trúc mở rộng

Thiết kế kiến trúc triển khai chuẩn

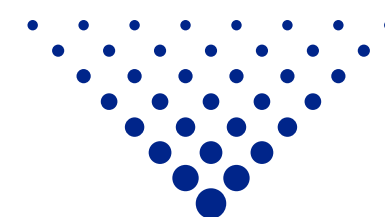
Tích hợp hệ thống, phân quyền truy cập, ghi vết và giám sát ngay từ đầu để AI vận hành ổn định ở quy mô lớn, giảm rủi ro phát sinh.



Vận hành & tối ưu dài hạn

Vận hành AI có kỷ luật chi phí

Theo dõi chất lượng, hiệu năng và chi phí theo tác vụ; tối ưu liên tục để đảm bảo hiệu quả đầu tư và tính bền vững khi mở rộng.



FPT Smart Cloud đồng hành cùng doanh nghiệp xây nền tảng Cloud và AI an toàn để tăng tốc chuyển đổi số bền vững.

Nguồn tham khảo:

- (1) <https://www.gartner.com/en/newsroom/press-releases/2025-10-22-gartner-forecasts-worldwide-it-spending-to-grow-9-point-8-percent-in-2026-exceeding-6-trillion-dollars-for-the-first-time>
- (2) <https://www.gartner.com/en/newsroom/press-releases/2026-1-15-gartner-says-worldwide-ai-spending-will-total-2-point-5-trillion-dollars-in-2026>
- (3) <https://our-thinking.nashtechglobal.com/insights/10-technology-trends-shaping-the-next-3-years>
- (4) <https://news.microsoft.com/source/features/ai/whats-next-in-ai-7-trends-to-watch-in-2026/>
- (5) <https://www.ibm.com/thought-leadership/institute-business-value/report/business-trends-2026>
- (6) <https://vneconomy.vn/tang-them-72-ty-usd-kinh-te-so-dong-gop-hon-14-vao-gdp-2025.htm>
- (7) https://services.google.com/fh/files/misc/vietnam_economy_sea_2025_report.pdf
- (8) <https://baochinhphu.vn/viet-nam-chinh-thuc-co-luat-tri-tue-nhan-cao-ai-102251210164948585.htm>
- (9) <https://mst.gov.vn/ai-va-co-hoi-vang-de-viet-nam-but-pha-trong-ky-nguyen-so-197251019190920487.htm>
- (10) <https://nguoiquansat.vn/552-000-cuoc-tan-cong-52-doanh-nghiep-viet-chiu-ton-hai-vi-tin-tac-nam-vung-269603.html>
- (11) <https://znews.vn/kip-thoi-xu-ly-vi-pham-sau-mot-thang-trien-khai-camera-ai-tai-ha-noi-post1617762.html>
- (12) <https://vnexpress.net/ap-luc-sau-ky-luc-xuat-khau-500-ty-usd-nam-2025-5002440.html>
- (13) <https://cafef.vn/nam-2025-thiet-hai-do-lua-dao-truc-tuyen-o-viet-nam-uoc-tinh-tren-6000-ty-dong-18826010807091841.chn>



Hotline: **1900638399**

Email: **fptsmartcloud@fpt.com**

Địa chỉ:

- Hà Nội: **FPT Tower, 10 Phạm Văn Bạch, Phường Cầu Giấy**
- TP. Hồ Chí Minh: **Tòa nhà PJICO, 186 Điện Biên Phủ, Phường Xuân Hòa**
- Tokyo: **33F, Sumitomo Fudosan Tokyo Mita Garden Tower, 3-5-19 Mita, Minato-ku**