10 TECHNOLOGY TRENDS IN VIETNAM

Opportunities to Accelerate in the Global Technology Wave

FPT Smart Cloud, FPT Corporation – February 2026

Global Technology Outlook in 2026

In 2026, AI enters the phase of large-scale operational deployment. The competitive landscape among enterprises will be defined by three core pillars: **Cloud infrastructure – Security – Governance.**

Systemic Technology Investment

According to Gartner, the global IT spending is projected to **grow by 9.8%**, surpassing **USD 6 trillion** for the first time[1]. Particularly, **global AI spending is expected to reach approximately USD 2.52 trillion by 2026**[2]. Enterprises are investmenting across multiple domains, including data, platforms, security, and infrastructure.

AI Agents: The Next-Generation Digital Workforce

Gartner forecasts, by 2029, **Agentic AI** will autonomously resolve 80% of customer service inquiries; thus, reducing 30% operational costs[3]. AI Agents are task-specialized and governed through identity management, access control, and strict data governance mechanisms, very much like human employees within the organization.

The Rise of Software Factories

GitHub reports **approximately 43 million pull requests per month** (a **23% year-over-year** increase) and **nearly 1 billion commits annually**[4]. These figures signal a fundamental transformation in the software industry, as AI becomes directly embedded in the way software is built, tested and improved, dramatically accelerating innovation cycles.

Digital Sovereignty: A Prerequisite for Scalability

According to IBM, **93% of executives state that Sovereign AI** will be a mandatory component of enterprise strategy by 2026[5]. Sovereign AI encompasses control over AI models and data security, enabling organizations to deploy AI at scale in a manner that is secure, compliant, and sustainable.

Key message: AI is evolving into a **foundational companion technology**, enabling enterprises to **operate more securely, maintain stronger control**, and **achieve more sustainable long-term operations.**

The State of Technology in Vietnam

By 2026, Vietnam will have converged sufficient driving forces to move AI from experimentation into real-world operations. The strategic shift centers on data optimization, system security, and purpose-driven AI deployment.

Rapid Expansion of the Digital Economy

Vietnam's digital economy continues to demonstrate strong momentum, with gross merchandise value (GMV) reaching **USD 72.1 billion** in 2025, representing a 14.6% growth rate[6]. This expanding scale is creating an urgent demand for intelligent operational automation across industries.

Digital Payments: A Primary Growth Engine

Digital payments act as the "circulatory system" of the digital economy and remain a key growth driver as the government accelerates the transition toward a cashless economy. This shift enables AI solutions to deliver value in reconciliation, security and financial risk management.

Users Are Ready for AI Agents

According to the Vietnam e-Conomy SEA 2025 report, 81% of users interact with AI on a daily basis and 96% are willing to share data with AI in exchange for personalized experiences[7]. This readiness places pressure on enterprises to build AI-powered solutions that ensure security, transparency and trust.

Government and Regulatory Momentum

The government is accelerating national data standardization and establishing new regulatory frameworks. The Artificial Intelligence Law, passed by the National Assembly and effective from **March 1, 2026**[8], provides a foundation for risk governance, controlled experimentation and safer large-scale AI deployment.

Key message: To realize AI at scale in Vietnam, enterprises must address three foundational challenges: Trusted Data - Compliant Security - Flexible Cloud Infrastructure.

Key Technology Trends for 2026

The strategic questions facing enterprises are increasingly centered on execution: How can AI be embedded into real operational workflows? How scalable are these deployments? How can risks be effectively governed?

Three Criteria Shaping Technology Trends in 2026:

Quantifiable Business Impact

Technologies must deliver measurable value, whether through productivity gains, cost optimization, or enhanced customer experiences.

Sustainable Operating Foundations

Trends are shaped by the convergence of Cloud Computing, Security, and Governance, forming a resilient and scalable operational backbone.

Feasibility in the Vietnamese Market

Solutions must be deployable within a 12-24 month timeframe, supported by momentum from the digital economy and local user behaviors.

*The more enterprises accelerate their AI adoption, the more critical it becomes to **advance innovation** in parallel with **stricter controls** over identity management, access rights, traceability and data protection.*

Associate Professor, Dr.
Ngo Xuan Bach
Director of AI Product Division, FPT Smart Cloud;
Director of the Quantum AI & Cybersecurity Institute, FPT Corporation

1 Multi-Agent Systems

What are Multi-Agent Systems?

Multi-agent systems (MAS) are composed of multiple autonomous AI Agents that interact within a shared environment to solve complex tasks that would be inefficient for a single agent to handle alone by dividing work, processing tasks in parallel and enabling collective learning and adaptation.

Agents operate in a task-oriented manner, including planning, tool invocation, system access (e.g., ERP/CRM), and workflow coordination to produce real-world, operational outcomes.

Growth Potential

MAS are expected to bloom in Vietnam driven by three key factors:

- **Pressure from the scale of the digital economy:** Enabling enterprises to automate end-to-end value chains, from logistics to payments.
- **Productivity optimization aligned with data sovereignty:** Allow enterprises to design controlled automation workflows that meet stringent security and compliance requirements.
- **A national AI ecosystem:** Create a favorable environment for AI deployment and supporting Vietnam's ambition to rank among the global top 50 AI-leading countries globally by 2030[9].

Practical Use Cases

Banking & Insurance

Coordinate between Business Assistant Agents and Fraud Detection Agents to trace transactions, detect anomalies and manage risk.

Retail & E-commerce

Optimize marketing campaigns, forecast demand and deliver omnichannel customer support.

Logistics & Manufacturing

Collaborate on production planning, predictive maintenance, and operational route optimization.

Public Services

Handle case routing, compliance verification, and service orchestration, enhancing transparency while reducing manual workloads.

Enterprise Perspective

Multi-agent systems represent a "new operating system" for digital enterprises, marking a shift from isolated AI solutions to coordinated teams of AI Agents. At FPT, FPT.AI delivers a comprehensive MAS solution set, enabling enterprises to operationalize AI across real-world business processes.

Orchestration Layer	Core System Integration	Enterprise-Grade Operations
Managing complex coordination and task execution across multiple agents.	Seamless API-based connectivity with existing CRM, ERP, and ITSM systems.	Built-in Observability, Governance, FinOps, and Audit Trails to ensure control, transparency, and cost efficiency.

To enable MAS deployment in sensitive data environments, we focus on

five foundational pillars across infrastructure and security:

1. **Compute Infrastructure:** Optimized for both AI training and inference workloads.
2. **Identity and Access Management (IAM):** Strict control over agents' data access scopes and permissions.
3. **Risk Governance Framework:** Ensuring compliance for industries with high regulatory barriers.
4. **Cross-System Orchestration:** API and workflow-based integration enabling end-to-end automation across core enterprise systems.
5. **Runtime Security for Agents:** Safety guardrails, approval mechanisms, and continuous monitoring for sensitive actions on cloud Infrastructure.

Pre-Deployment Recommendations

- ☑ **Standardize authority and permissions:** Clearly define agent identities and limit access rights based on explicit governance principles.
- ☑ **Separate orchestration from execution layers:** Enable control, logging (logs/audit trails), and approval workflows for critical actions.
- ☑ **Measure against business objectives:** Establish KPIs for processing time, error rates, compliance levels, and conduct testing against potential attack scenarios.

Key Message

Success with multi-agent systems depends not only on technology, but also on how enterprises govern and manage a digital workforce. FPT.AI, through the FPT AI Agents suite, partners with enterprises to optimize systems, ensure secure operations, and unlock the full potential of AI at scale.

Associate Professor, Dr.

Ngo Xuan Bach

Director of AI Product Division, FPT Smart Cloud;
Director of the Quantum AI & Cybersecurity Institute, FPT Corporation

2 AI-Native Development Platforms

What are AI-Native Development Platforms?

AI-native development platforms represent a new generation of software development platforms where AI is embedded as a core component, actively participating throughout the entire software development lifecycle, from system design, coding, testing, and debugging to documentation and system operations.

By automating repetitive and time-consuming tasks, AI enables engineers to focus on architectural thinking and solving complex business problems rather than routine execution.

Growth Potential

AI-native development platforms significantly shorten feature release cycles, standardize software quality, and mitigate risks associated with embedding AI into development workflows.
Vietnamese enterprises are expected to transition toward AI-native development models driven by four critical factors:

- Rising digital competitiveness, forcing faster feature delivery within shorter timeframes.
- Widespread internet and 5G infrastructure, combined with the rapid expansion of digital services, increasing system scale, and development velocity pressure.
- The need for standardized development processes, from design and testing to deployment, enabling speed without compromising reliability.
- Centralized governance, including identity management, access control, data protection, and auditability to ensure security and compliance.

Practical Use Cases

Banking & Finance

Automated test generation, security vulnerability scanning and accelerated feature releases.

Retail & E-commerce

Development of promotion engines and dynamic pricing systems; operational support and incident alerting.

Manufacturing & Logistics

Rapid development of warehouse management, maintenance, and operational monitoring applications.

Public Administration

Standardized documentation, operational logs and automated testing for digital public service portals.

Enterprise Perspective

With the goal of enabling enterprises to accelerate development while maintaining operational control, we are building next-generation AI platforms alongside a cloud ecosystem deeply integrated with security and governance.

- **Isolated Environments:** Ensure enterprise source code is trained and suggested within secure zones (Private/Hybrid Cloud).
- **Internal Developer Platform (IDP):** Enable developers to access AI resources in a governed and secure manner with a standardized internal platform.

FPT.AI's Deployment Model

Layer 1: Platform Standardization

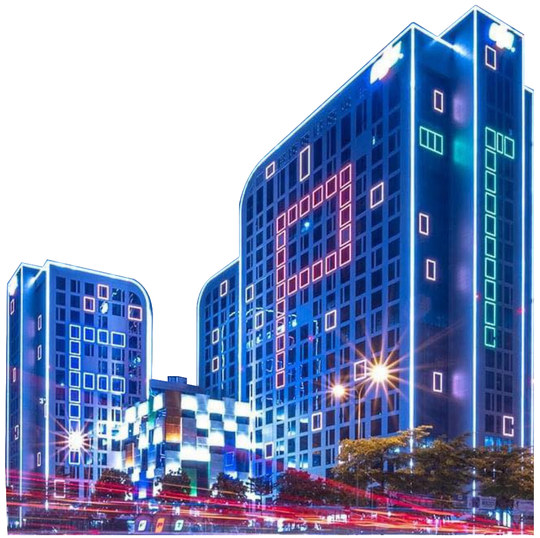
Establish code repositories, CI/CD pipelines and centralized monitoring systems.

Layer 2: AI Augmentation

AI integration into resource-intensive tasks such as documentation, test generation, and security scanning.

Layer 3: Governance & Compliance

Output quality measurement using real operational metrics, with full traceability of AI actions.

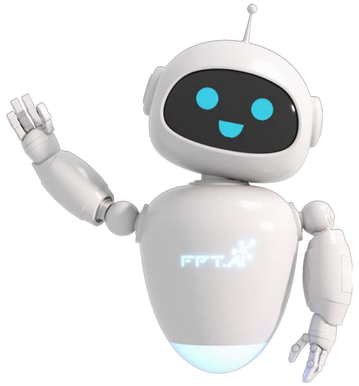


Pre-Deployment Recommendations

- ☑ **Protect source code:** Prevent sensitive data leakage by deploying AI in isolated environments; avoid exposing proprietary code to public models.
- ☑ **Enforce control standards:** AI-generated code must undergo strict logic review; AI may compile successfully but still produce subtle errors without governance.
- ☑ **Secure the software supply chain:** Be cautious of third-party libraries that may contain malicious code unintentionally suggested by AI.
- ☑ **Ensure auditability:** Maintain complete audit trails of AI decisions to support incident investigation and software

Key Message

With FPT's product and solution ecosystem, we combine cloud infrastructure, deep implementation services and enterprise-grade operating processes to help enterprises move rapidly from experimentation to real-world AI operations.



3
AI Factory - Computing Infrastructure for AI

What is an AI Factory?

An AI Factory is a specialized cloud infrastructure designed specifically for AI workloads. It uses next-generation GPUs as its computational core, integrated with storage and AI operating software to support a closed-loop lifecycle, from training and fine-tuning to large-scale deployment and inference. AI factories are regarded as the new infrastructure standard of the AI era.

Growth Potential

- **Exploding demand for data and model processing:** As enterprises accelerate digitalization and automation, AI compute demand grows rapidly, requiring centralized "factory-style" architectures instead of fragmented, project-based deployments.
- **AI Sovereignty and Geopatriation:** Processing is shifting from global cloudsw to regional or national infrastructure to reduce geopolitical risk and enhance data control, making sovereign, domestic AI Factories ideal for sensitive data.
- **AI Cost Discipline (FinOps):** GPU and model operating costs are increasingly governed through financial operations, measured per task, department, and business outcome.
- **Energy Efficiency:** Rising power and data center operational costs push enterprises toward hybrid cloud architectures, higher compute density, and reduced resource waste..

Practical Use Cases

Sovereign AI Infrastructure

Help governments build domestic AI capabilities, develop AI models with local data and language, promote economic growth, and elevate national positioning in the AI field.

Advanced Robotics & Automotive

Provide high-performance computing and real-time data processing capabilities to train AI models, automate manufacturing and improve accuracy and safety of autonomous vehicles.

Drug Discovery & Personalized Medicine

Analyze big data and apply generative AI to discover new drug molecules, develop personalized treatment protocol, improve treatment effectiveness and reduce expenses.

Intelligent & Safe Financial Services

Detect fraud transactions, optimize banking customer service and utilize algorithmic trading with robust, comprehensive AI infrastructure.

Enterprise Perspective

In Vietnam, FPT Smart Cloud, a member of FPT Corporation, is the first and only provider to systematically deploy AI Factory Infrastructure, in collaboration with global partners such as NVIDIA.

FPT positions AI Factory as a shared national platform, supporting sovereign AI and infrastructure geopatriation:

Flexible compute resources: GPU Cloud/GPU clusters for training and inference, supporting a multi-tenant mechanism for performance optimization.

Standardized model operations: CI/CD pipelines for models, model registries, automated monitoring, and traceability.

AI FinOps: Real-time cost tracking by task and business unit, enabling transparent ROI measurement.

Pre-Deployment Recommendations

- **Cost risk management:** Idle or poorly allocated GPUs can become budget "black holes". Intelligent resource orchestration is critical.
- **Data governance:** Unstandardized data leads to "garbage data." A clean data filtering layer is required before entering the AI factory.
- **Zero-trust security:** Models and training data are critical assets and must be protected with strict IAM and audit trails.

Key Message

Utilize AI Factory as a strategic platform to develop, implement and scale AI with speed, flexibility and compliance.

4 Domain-Specific Language Models (Vertical LLMs)

What are Domain-specific Language Models?

Domain-specific language models (DSLMs), also known as **Vertical LLMs**, are language models trained deeply for specific industries such as finance, healthcare, legal, or manufacturing.

Unlike general-purpose LLMs that provide broad but often generic responses, DSLMs are trained on domain-specific data, terminology and workflows, resulting in higher contextual understanding, reduced hallucination and stronger compliance.

Growth Potential

By 2026, Vietnamese enterprises are shifting toward 'Responsible GenAI,' making DSLMs essential due to 3 core values:

- **Accuracy and reliability:** Deep understanding of domain abbreviations, technical symbols and legal frameworks (e.g., the Vietnamese Civil Code).
- **Security and privacy:** DSLMs are often trained on private infrastructure to prevent sensitive business knowledge leakage.
- **Cost and performance optimization:** Smaller, specialized models (SLMs) deliver superior performance in narrow domains at lower infrastructure costs.

Practical Use Cases

DSLMs are particularly suited for industries requiring high accuracy and compliance

Enterprise Perspective

Recognizing that each industry has unique language, workflows and compliance requirements, **FPT** positions domain-specific models as a core enterprise capability, **transforming internal knowledge into competitive advantage.** To date, FPT.AI has **developed over 50 domain-specific language models,** enabling faster deployment, higher accuracy and better risk control at scale.

For DSLMs to transit from "model" to "operational capability," we focus on

three cross-cutting capabilities:

GPU Cloud infrastructure (FPT AI Factory)

Ensuring sufficient compute for training, fine-tuning and enterprise-scale deployment.

Agent quality flywheel

Automated data → training → evaluation → deployment → continuous improvement loops.

Domain knowledge systems

Ensuring models understand enterprise language consistently through knowledge bases and standardized taxonomies.

Pre-Deployment Recommendations

- ☑ **The "Garbage In, Garbage Out" principal:** Poor domain data leads to incorrect learning - knowledge must be standardized before training.
- ☑ **Source citation mechanisms:** Combine DSLMs with RAG architectures to ensure traceable internal document references.
- ☑ **Bias monitoring:** Periodic evaluation and industry-specific benchmarks are essential.
- ☑ **Long-term operating costs:** Fine-tuning and maintenance are resource-intensive; start with high-ROI use cases.

Key Message

In the AI era, competitive advantage lies not in owning technology, but in owning models that deeply understand your enterprise's knowledge and data.

5
AI Governance & AI Security Platforms

What are AI Governance and AI Security Platforms?

To operationalize AI in real-world environments, enterprises must combine AI Governance and AI Security Platforms in a complementary manner:

- **AI Governance:** A set of principles and mechanisms for managing the AI lifecycle (from Data – Models – Agents), defining which data may be used, role-based access rights, requirements for controlling bias and hallucinations and maintaining audit trails to demonstrate compliance.
- **AI Security Platforms:** Systems designed to protect against security risks when deploying AI, including prompt injection attacks, data leakage through system logs, abuse of privileges by AI agents and risks arising from the AI model supply chain.

Growth Potential

2026 marks an inflection point for AI Governance demand as risks shift from "incorrect answers" to "incorrect actions."

- **Regulatory momentum: Personal Data Protection regulations** introduce new requirements for sensitive data governance. AI Security and Governance become mandatory compliance infrastructure.
- **Cybersecurity reality:** With more than **552,000 cyberattacks** recorded in Vietnam in 2025[10], AI inadvertently expands the attack surface. Enterprises require continuous monitoring mechanisms rather than periodic assessments.
- **Global standardization pressure:** Regulations such as **the EU AI Act** impose high-risk AI governance requirements, compelling Vietnamese enterprises to prepare equivalent control mechanisms when working with EU markets and partners.

Practical Use Cases

Banking & Finance

Control credit model risks, maintain full audit trails of AI decisions for accountability & financial fraud prevention.

Retail & E-commerce

Prevent AI from fabricating policies or leaking customer purchase histories.

Healthcare

Establish data protection guardrails, enforce role-based access control (RBAC) for medical records, and ensure strict auditing.

Public Administration

Prevent fabricated regulations, ensure knowledge accuracy and maintain verifiable information sources.

Enterprise Perspective

At the enterprise level, risk concentrates around access rights, actions, and legal liability. Therefore, AI deployment must incorporate governance and security from the very first step.

We recommend a five-layer framework:

1. **Data classification:** Identify sensitive data and define permissible ai usage scopes.
2. **Risk classification:** Assess the impact level of each specific use case.
3. **Identity and access management (IAM):** Enforce strict access control for users and agents.
4. **Runtime monitoring:** Track access, actions, output quality and model drift in real time.
5. **Proactive defense:** Block prompt injection attacks and prevent data leakage.

In practical deployments, we focus on three core capabilities to help enterprises scale AI rapidly while retaining control over data, agent behavior, and legal risk:

Audit Trail	Red Teaming	Domestic Cloud Platforms
Traceability and compliance support.	Attack testing prior to go-live.	Support data sovereignty and reduce dependency on cross-border infrastructure.

Pre-Deployment Recommendations

- ☑ **Avoid superficial governance:** Policies without logging and audit tools cannot control real risks.
- ☑ **Balance control and innovation:** Overly strict controls push employees toward Shadow AI. Risk-based tiering is required.
- ☑ **Prevent agent privilege abuse:** Every AI Agent must be identified and granted limited authority, similar to a real employee.
- ☑ **Human-in-the-loop mechanisms:** Establish human approval points for sensitive actions (fund transfers, data deletion, etc.).

Key Message

Do not wait for incidents to secure AI. An AI system without governance is like a race car without brakes: The faster it goes, the greater the danger. FPT provides the safety brakes that allow enterprises to accelerate with confidence.

6 Preemptive Cybersecurity

What is Preemptive Cybersecurity?

Preemptive cybersecurity is a proactive, automation-driven approach that continuously tests, predicts and prevents threats before damage occurs. Instead of reacting after incidents, this model integrates **offensive testing** into daily operations.

It focuses on three capability layers:

- **Early detection:** Continuous monitoring to identify even minor anomalies.
- **Correct prioritization:** Risk scoring to focus on vulnerabilities with the greatest potential impact.
- **Automated response:** Isolation, blocking or recovery through controlled scenarios.

Growth Potential

In 2026, preemptive cybersecurity will become essential in Vietnam due to:

- **Rising real-world incidents: 552,000 cyberattacks** were recorded in Vietnam, with 52.3% of organizations breached at least once. Periodic assessments can no longer keep pace with expanding attack surfaces.
- **Talent shortages:** Nearly **48%** of organizations lack dedicated cybersecurity staff[10], forcing **automation** of detection and response to maintain security level.
- **Explosion of AI Agents:** Operational AI agents must be identified, authorized, and protected as risk-bearing identities.

Practical Use Cases

Banking & Finance

Automate incident detection and response; abnormal access blocking; real-time protection of digital identities and transactions.

Retail & E-commerce

Block data-scraping agents, prevent customer data leaks and monitor sophisticated promotion fraud.

Manufacturing & Logistics

Monitor IoT/OT risks, detect malware infiltration early and prevent operational disruption.

Public Administration

Protect sensitive citizen data; early intrusion alerts and full forensic logging.

Enterprise Perspective

At FPT, FPT Smart Cloud integrates preemptive cybersecurity into FPT Cloud and FPT.AI, enabling early threat detection.

We enable proactive security based on **three foundational pillars:**

Threat Intelligence

AI continuously scans data to identify emerging attack patterns and update defensive rules.

Autonomous Threat Hunting

Security AI agents conduct authorized simulations, detect weaknesses, propose remediation and automatically patch vulnerabilities.

Behavioral Analytics

Abnormal access patterns trigger immediate isolation to prevent damage propagation.

By embedding cybersecurity capabilities into FPT Cloud, we help enterprises automate incident response, implement security from the design stage and block attacks early before they spread.

Pre-Deployment Recommendations

- **Trust thresholds:** Include approval mechanisms for sensitive actions in automated responses to avoid unintended disruptions.
- **Reduce alert noise:** Prevent alert fatigue by prioritizing vulnerabilities that directly impact business logic.
- **Privacy protection:** Align deep monitoring with data classification and the principle of least privilege.

Key Message

In the AI era, security must stay ahead of risk. FPT helps enterprises detect early – prevent early–respond automatically, ensuring secure and compliant AI deployment.

7 Computer Vision & Vision Agents

What are Computer Vision & Vision Agents?

In 2026, **computer vision** evolves beyond "seeing and recognizing" into **Vision Agents** - systems capable of observing, reasoning in context, and executing tasks within business workflows.

- **Computer Vision** processes images and video to extract structured information (objects, defects, behaviors, text, etc.).
- **Vision Agents** are complete "AI workers," combining computer vision with **vision language models** (VLMs) to not only 'see' but also '**understand**' context. Vision Agents can plan actions, invoke APIs and execute decisions aligned with business objectives.

Within MAS, Vision Agents act as "scouts," observing reality, converting visual data into digital signal, and triggering coordinated actions across agents.

Growth Potential

Vietnam's market presents three accelerating factors:

- **Rising automation demand:** Enterprises seek productivity gains without relying solely on Cloud connectivity due to latency and availability constraints.
- **Smart City development:** Hanoi and Ho Chi Minh City operate thousands of AI cameras; Hanoi alone detected over **6,300 traffic violations** via AI-based enforcement[11].
- **Edge AI maturity:** On-device image processing reduces latency, bandwidth load and keeps sensitive data local.

Practical Use Cases

Vision Agents are subject to deployment as 4 core solution sets:

Manufacturing & Warehousing

Visual defect inspection; workplace safety monitoring and emergency alerts.

Retail & Customer Experience

Empty-shelf detection; heatmap analysis to optimize layouts and customer flow.

Public Services & Finance

eKYC, deepfake detection; invoice and document data extraction.

Healthcare

Patient monitoring and alerts, reducing supervision burdens on medical staff.

Enterprise Perspective

FPT approaches Vision Agents as an operational deployment challenge, built on **three core capabilities:**

Flexible infrastructure

Deploy across both Cloud platforms and Edge AI for real-time image processing.

Proven vision solutions

Leverage deployed capabilities such as eKYC, OCR, and image analytics modules.

Workflow integration

Connect cameras/IoT with business systems (alerts, processing, reporting), including access control and audit trails.

Pre-Deployment Recommendations

- **Prioritize privacy:** Collect images only for defined purposes; enforce strict access control and comprehensive audit trails.
- **Context-aware accuracy control:** Lighting, angles and occlusion affect accuracy; hence, input standardization and periodic model validation are required.
- **Optimize storage costs:** Process video at the edge and upload only necessary data to reduce bandwidth and cloud storage costs.

Key Message

In 2026, data appears everywhere through camera lenses. Enterprises that can "see" and process visual data fastest will dominate on-the-ground operations.

8
Physical AI

What is Physical AI?

Physical AI refers to AI systems capable of perceiving, reasoning, deciding and executing actions directly in the physical world. It combines robots, sensors, automation systems and digital twins to simulate, monitor and optimize real-world operations.

Unlike Generative AI, which processes digital data, physical AI operates in a closed loop:

Perception → Reasoning → Decision → Action

Growth Potential

In 2025, **Vietnam's exports** reached approximately **USD 475 billion**[12], with sustained FDI inflows, creating favorable conditions for **physical AI adoption.**

- **Labor pressure and safety:** Automating heavy, repetitive or hazardous tasks.
- **Export manufacturing competitiveness:** Higher yield rates, reduced downtime, optimized production lines.
- **Abundant field data:** Sensor networks and operational systems provide real-time inputs for AI control.

Practical Use Cases

Physical AI is fostering transformation in Vietnam's core industries:

Smart Manufacturing

Collaborative robots (cobots) for assembly, inspection, and handling.

Logistics & Warehousing

AGV/AMRs optimizing routes, avoiding obstacles and coordinate in fleets to improve processing speed.

High-Tech Agriculture

Robots and sensors detect crop maturity and identify diseased areas to enable precision spraying or harvesting, reducing material waste and labor costs.

Infrastructure & Urban Systems

Real-time monitoring systems detect early signs of electrical failures, substation incidents, fire risks, or structural damage, enabling timely intervention.

Enterprise Perspective

In the future, physical AI will become a critical building block of the broader AI-nation ecosystem. Its value is maximized when deployed using a "field-to-center" architecture, meeting real-time requirements at the edge while enabling centralized governance of data, models and operations.

Edge processing

Run inference directly at factories or warehouses to ensure low latency and stable operation during connectivity disruptions.

Cloud platform for training & operations (AI Factory)

Centralize large-scale data for training, simulation via Digital Twins and full MLOps lifecycle management.

Industrial integration

Connect AI systems with PLC/SCADA and enterprise platforms such as ERP, MES, and WMS to embed AI into real operational workflows.

With GPU computing infrastructure, model governance platforms, and deep system integration capabilities of FPT Smart Cloud, together with the FPT technology ecosystem, enterprises can deploy physical AI with a clear roadmap:

Effective at the field → Governed at the center → Scalable across operations.

Pre-Deployment Recommendations

- **Model-to-field gap:** Environmental factors such as lighting changes, dust, and vibration can cause model drift. Continuous monitoring and periodic recalibration mechanisms are required.
- **IT-OT integration:** Connections between IT systems and operational technology (OT) must be segmented and secured using Zero Trust principles to prevent lateral attacks.
- **Behavioral guardrails:** AI systems controlling physical assets must include hard-stop safety mechanisms and exception-handling scenarios to protect human operators.
- **Pragmatic ROI focus:** Start with clearly defined pain points - such as defect reduction or energy optimization, rather than broad, factory-wide deployments.

Key Message

If multi-agent systems are the digital operating system, physical AI is the execution arm. Together, they enable enterprises to automate production lines and logistics operations, supporting the transition from low-cost manufacturing to intelligent, autonomous production.

9
Digital Provenance & Content Integrity

What are Digital Provenance & Content Integrity?

Digital Provenance and **Content Integrity** form a complementary technology stack that verifies **the origin and integrity of digital content**, identifying who created it, when it was created, how it was created (AI or human) and whether **it has been altered after publication.**

- **Digital Provenance:** Records the content's lifecycle (creation, modification, publication) using metadata, cryptographic signatures, hashes and optionally watermarking to identify AI-generated or AI-modified content.
- **Content Integrity:** Detect and alert on unauthorized changes. Any mismatch in digital signatures or hash values triggers alerts for potential tampering.

Growth Potential

As deepfakes become increasingly difficult to detect visually, content authenticity has become mission-critical in Vietnam:

- **Fraud and impersonation prevention:** In 2025, Vietnam incurred an estimated **VND 6 trillion** in losses from online fraud[13]. Digital Provenance enables content verification for eKYC, customer service and brand communications.
- **Regulatory compliance:** New regulations emphasize transparency and risk governance for AI-generated content. Provenance mechanisms provide verifiable content history for compliance.
- **International standardization:** Frameworks such as **C2PA** are increasingly adopted by global technology and media companies. Vietnamese enterprises working with international partners must comply with these standards to protect digital assets and brand reputation.

Practical Use Cases

BFSI

Prevent forged contracts and records; verify data sources used in credit scoring models.

Public Administration

Authenticate official documents and public announcements; reduce misinformation risks.

Marketing

Label and manage AI-generated content; prove content authenticity to protect brand equity.

Multi-Agent Systems

Verify agent-generated content before downstream processing in large-scale automated systems.

Enterprise Perspective

To operate AI at scale, enterprises need a **trust layer** that **verifies content origin, ensures integrity, and enables accountability**; therefore, reducing impersonation, misinformation, and data leakage risks.

We recommend a three-layer implementation approach:

Layer 1: Trusted Infrastructure

Immutable storage, centralized key management, access control, and comprehensive logging.

Layer 2: Content Authentication

Apply C2PA standards, digital signatures, and time-stamping to prove authorship, creation time, and integrity.

Layer 3: Secure Operations

Integrate deepfake detection, distribution channel monitoring, and incident response workflows.

When integrated into the FPT ecosystem, the **trust layer** enables enterprises to:

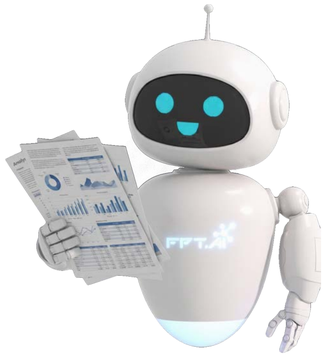
- **Control data and model provenance within the AI factory:** Manage MLBOM (Machine Learning Bill of Materials) to reduce model supply-chain and data contamination risks.
- **Protect intellectual property:** Prove ownership of data and content, support dispute resolution, and prevent unauthorized data extraction for training.

Pre-Deployment Recommendations

- ☑ **Provenance loss risks:** Metadata can be lost through screenshots, compression or unsupported platforms. Combine in-file provenance with digital signatures, time-stamping and approval workflows.
- ☑ **Define clear signing points:** Specify where signatures are applied (input data, training data, or published outputs), who is responsible and under what criteria, which are critical for audits.
- ☑ **Not a replacement for cybersecurity:** Provenance validates authenticity but does not replace fraud prevention, access control, monitoring or crisis response mechanisms.

Key Message

In the era of AI-generated content, provenance and integrity verification are foundational requirements for secure and trustworthy digital operations.



10 Quantum Computing

What is Quantum Computing?

Quantum Computing uses **qubits** instead of classical 0/1 bits. Leveraging physical phenomena such as **superposition** and **entanglement**, quantum systems solve certain problems, especially optimization, material simulation, chemistry and cryptography, in fundamentally different ways from classical computers.

From 2026 onward, major players such as IBM and Microsoft are expected to move from research into structured, planned deployments, particularly for simulation and cryptographic security use cases.

Growth Potential

Quantum Computing in Vietnam is transitioning from theory to action:

- **Policy direction:** Vietnam officially designated Quantum Computing as a strategic technology under **Decision 1131/QĐ-TTg (06/2025)**, establishing a framework for 2026 - 2030.
- **Growing expert community:** The VNQuantum network, launched in 08/2025, connects over **2,000 experts** from 22 countries, supporting research and experimentation.
- **Enterprise investment:** FPT established the Quantum AI & Cybersecurity Institute (QACI) with a **USD 100 million** investment, signaling leadership in quantum research and applications.

Practical Use Cases

Banking & Finance

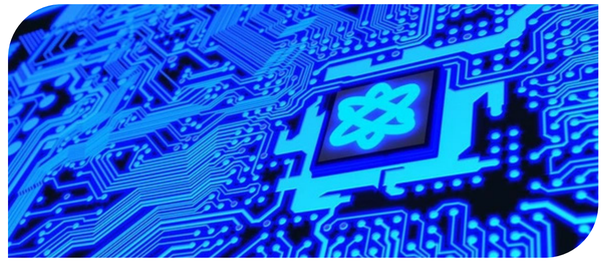
Ultra-fast portfolio optimization, risk management, and liquidity modeling.

Manufacturing & Logistics

Optimization of production schedules, resource allocation, and transportation routes.

Healthcare & Energy

Molecular and material simulation to accelerate R&D; power grid optimization and load balancing.



Enterprise Perspective

In 2026, Quantum Computing in Vietnam will remain largely in the research and pilot phase. Enterprises should prepare strategically to capture value as the technology matures.

Three practical paths for research and experimentation:

Select the right problems

Focus on optimization and simulation tasks with clear quantum advantage.

Design hybrid architectures

Use classical HPC for data processing and simulation, while experimenting with Quantum Cloud services for optimization cores.

Prepare for post-quantum security

Plan migration to Post-Quantum Cryptography (PQC) for systems requiring long-term data protection.

Pre-Deployment Recommendations

- **Do not build your own quantum computer:** Quantum infrastructure requires specialized conditions and high costs. Use quantum cloud services or partner-led pilot programs.
- **Develop talent and capabilities:** Quantum engineers and hybrid system architects are scarce; invest in training, hiring or research partnerships.
- **Information security risks:** Long-lifecycle data (e.g., finance, healthcare) must transition to quantum-resistant encryption to mitigate future decryption risks.

Key Message

Start with focused pilots, measurable KPIs and build internal capabilities in data, algorithms, and cybersecurity to be ready when the market matures.

Associate Professor, Dr.

Ngo Xuan Bach

Director of AI Product Division, FPT Smart Cloud;

Director of the Quantum AI & Cybersecurity Institute, FPT Corporation

Next Steps for Enterprises

From strategy to execution to scale AI securely, measurably and cost-effectively.

Assess & standardize

Build a strong AI foundation
Evaluate readiness across data, infrastructure, security and operations to identify gaps and remediation roadmaps.

Prioritize the right use cases

Adopt use cases for immediate business impacts
Select scenarios with available data, clear workflows and measurable KPIs to generate early wins.

Design for scale

Implement scalable architecture from day one
Integrate systems, enforce access control, auditing and monitoring to ensure stable large-scale operations.

Operate & optimize long-term

Apply AI FinOps discipline
Continuously track quality, performance and cost per task toensure sustainable ROI.

FPT Smart Cloud partners with enterprises to build secure Cloud and AI foundations - accelerating sustainable digital transformation.

References

(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_e_conomy_sea_2025_report.pdf

(8) https://baochinhphu.vn/viet-nam-chinh-thuc-co-luat-tri-tue-nhan-tao-ai-102251210164948585.htm

(9) https://mst.gov.vn/ai-va-co-hoi-vang-de-viet-nam-but-pha-trong-ky-nguyen-so-19725101919092048 7.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

FPT Smart Cloud

Hotline: **1900638399**

Email: **fptsmartcloud@fpt.com**

Address:

- Tokyo: **33F, Sumitomo Fudosan Tokyo Mita Garden Tower, 3-5-19 Mita, Minato-ku**
- Hanoi: **No. 10 Pham Van Bach Street, Cau Giay Ward**
- Ho Chi Minh City: **PJICO Building, 186 Dien Bien Phu Street, Xuan Hoa Ward**