Deep Science Publishing, 2025
https://doi.org/10.70593/978-93-7185-625-6_4

DeepScience
Open Access Books

Chapter 4: Integrating IoT and Connected Devices into Enterprise-Grade AI Platforms

4.1. Introduction

Enterprises can manage AI applications in production by leveraging both the Google Cloud Platform (GCP) and Google's private computing platform. An enterprise-grade AI platform requires more than just TensorFlow and CPUs: scalable training in the cloud is a necessity. GPUs speed up training throughput by so much that an enterprise might even consider renting GPUs instead of buying them. The next logical step is to rent an entire TPU pod, which costs millions of dollars, typically unimaginable for all but the most groundbreaking projects.

Beyond training, scalable prediction is equally essential. A hosted model offering adjusts scale in line with user demand. Moreover, enterprises must oversee continuous deployments, testing current model versions with production traffic. Continuous training is equally vital, combining existing data sets with fresh data. In this approach, fresh data (often from "Internet of Things"-enabled devices located in the wild) enables models that constantly adapt to distribution changes or concept drift.

4.1.1. Purpose and Scope of the Study

Connected devices and Internet-of-Things (IoT) technologies are becoming central to digital transformation initiatives of enterprise organizations. They provide tremendous amounts of data that can lead to valuable insights and actionable intelligence about how businesses operate and what customers need. AI has emerged as one of the leading ways to optimize business functions, grow and expand into new markets, improve customer experience, and deliver better outcomes.

To meet the strategies of an enterprise-scale AI solution, a platform should support a variety of input data types, sources, and endpoints, provide adequate storage and compute resources for the processing of information, offer broad access to data assets,

and support a comprehensive set of analytic and AI model types and requirements. In addition, a platform should support cross-team collaboration and enable the generation, deployment, management, and governance of business models through integrated and embedded AI capabilities.

4.2. Understanding IoT and Connected Devices

The term Internet of Things (IoT) has become a household term, encompassing everything from the newest Fitbit to the iPhone that everyone seems to have smartly attached to their wrist to the newest Google Home device and Alexa connected to your voice. One definition that helps understand IoT in the enterprise context is "A network of physical objects or 'things' embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data." These connected devices provide targeted intelligence to help support business operations and manage risks ranging from remote workforce safety to supply chain resiliency.

There are many benefits to IoT devices in a business setting: they provide added visibility and insights into situations that otherwise might have been impossible to have had any awareness or insight; enable data-driven, fact-based decisions rather than relying on intuition; inform better business outcomes; and manage losses by recognizing and predicting issues and risks [1-3]. But these IoT devices—even if deployed in an enterprise context—have been built in companies not experienced in enterprise software development and are not designed to scale with enterprise needs. Most enterprises realize that these consumer applications do not meet their needs and requirements. That is why most businesses still rely on spreadsheets to track and manage their operations and risks.

4.2.1. Definition and Scope

The Internet of Things (IoT) is a hub linking things, people, and processes through a unique identification and addressing scheme to enable intelligent decision-making [10], which, by 2020, will consist of 20 billion connected things [9]. Mobile devices already add intelligent capabilities, responsive to local contexts and locations. The IoT will contribute by expanding sensing and access to information about the surrounding environment and conditions. Monitors and controls can be integrated into homes, cities, electrical grids, transportation systems, and any other physical context. Intelligent capabilities encompass not only awareness but also autonomy in acting for specific purposes. Examples include traffic lights that converge traffic streams to a traveler's car, thermostats that optimize climate control based on outside weather conditions and building occupancy, personal health monitors that warn about an impending heart attack, and refrigerators that detect a spoiled item.

Although IoT will introduce myriad small devices capable of varying degrees of autonomous decision making, a layered, intelligent processing model distinguishes between appropriate levels of intelligence at the edge versus the core. Processing at the edge is supported by a locally constrained but intelligent environment that includes (millions of) small and simple decision points acting both autonomously and in cooperation within their constrained scope and (hundreds of) more powerful computational centers capable of providing a larger context for those devices. Then, a more general-purpose decision level takes into account even broader considerations and may even modify lower-level rules to affect behavior probing. Supervised learning at the lower level may narrowly focus on site-specific rules, while at the higher level, it involves larger-scale learning based on the combined historical activities of thousands or millions of homes in multiple contexts. Due to the wide breadth of different activities creating widely ranging types of information, it is not feasible to find reasons to answer queries, which is why high-performance machines are necessary to choose the right purpose, the right information, and the right context. Therefore, a layered intelligence model calls for an intelligent IoT infrastructure.

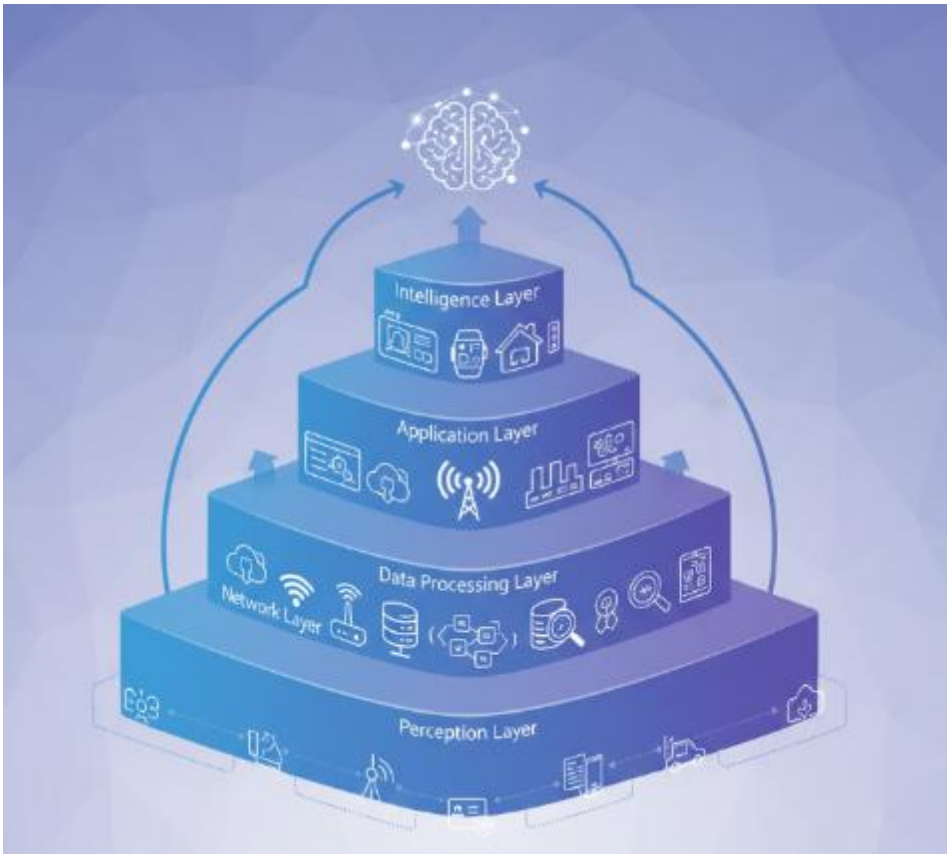

Fig 4 . 1 : The Internet of Things (IoT): A Layered Intelligence Model

4.2.2. Key Technologies in IoT

The fingerprint sensor represents a typical IoT device; it identifies the fingerprint of a finger press and sends the data to the cloud for AI platform processing. The AI platform Cloud Flutter SDK, deployed on the cloud, provides a lightweight way to collect, display, and play data. The Cloud Flutter SDK decodes data from a specific device—it supports decode functions for multiple devices, including PCs and mobile phones. The Flutter SDK is Mint's cross-platform development framework. The fingerprint sensor, for example, serves as a miniature server—it provides endpoint data to Flutter for decoding. Flutter interprets the data and passes its contents, including images or text, to the hosting device; the code running there can use this information as needed. The cloud is also responsible for data storage and monitoring.

Each device is accompanied by a Console, which offers comprehensive control over the device's operation and communication with other devices. This Console initiates the endpoint for Cloud Flutter SDK data decoding. The cloud backend, implemented using the BanMoBA framework, supports multiple devices simultaneously, as these devices can execute numerous tasks concurrently. Mint supports the entire development lifecycle, from writing code to defining strategies and building backend systems, thereby simplifying development and expediting delivery.

4.2.3. Challenges in IoT Implementation

The challenges of implementing IoT systems are indeed complex and remain challenging. Sensors attached to home appliances and on human and animal bodies, generating huge volumes of IoT data, create substantial problems of data management and analysis.

Every product connected to the Internet has an IP address, facilitating traceability from manufacturer to user [2-4]. This traceability benefits companies by providing a complete satisfaction curve, but also exposes IT systems to numerous hack attacks and cyber intrusions. The involvement of multiple actors and the rapid advances in technology further complicate IoT applications, calling for advanced security management.

4.3. Overview of AI Platforms

Enterprise AI platforms combine a range of common AI technologies and capabilities to enable organizations to build their own enterprise-grade AI applications. Such applications typically integrate with the Internet of Things (IoT) and connected devices and operate on an enterprise scale.

In examining the integration of information generated from the real world with information technology systems, there is a natural division. Real-world objects need to be sensors that capture and respond to information, and need to be actuators that respond to changes in the state of physical inspection. The results of their sensing need to be captured and encrypted so that information coming from the real world can be integrated and displayed with other enterprise information. All of that must be accomplished in a secure and appropriate management environment. To understand how to build and operate a world-class connected devices business, it helps to explore these enabled ecosystem elements.

4.3.1. What Constitutes an AI Platform?

The term AI platform is frequently mentioned but seldom clearly defined. AI itself is a broad concept that entails many capabilities. In 2012, IBM Watson was still an ASR, NLP, KRR, and TM system, including an NN for QA. Since then, countless other platforms have emerged, each characterized by specific AI technologies that underpin the brands, functions, and accomplishments promoted by their providers. Within the enterprise sector, such platforms extend far beyond the mere definition of AI or ASR, NLP, KRR, TM, and NN.

An AI platform caters to enterprise needs. It is a comprehensive IT enterprise offering, chiefly cloud-based, that encompasses a multitude of AI capabilities. The inclusion of IoT sensors and connected surveillance devices within an enterprise-grade AI platform for city, community, and building management is thus warranted.

4.3.2. Types of AI Platforms

Today’s AI platforms can be categorized according to specific enterprise AI infrastructure and service needs.

AI development platforms provide developers with AI-specific services that can be integrated into enterprise systems. These tools assist in building, training, testing, and deploying AI models for various applications and industries, enabling AI adoption.

AI-enabling infrastructure platforms combine the capabilities of AI development platforms with providing the underlying infrastructure for training and running AI application models. They provide the necessary hardware resources—such as CPUs, GPUs, TPUs, and networking elements—either in a public cloud or through private infrastructure.

Enterprise AI platforms constitute the overarching AI architecture for an enterprise, enabling the implementation and execution of company-wide AI initiatives. An enterprise AI platform integrates AI development and infrastructure platforms via APIs and connectors. This integration allows enterprises to source AI models from internal teams or external parties—whether hosted in the public cloud or in on-premises AI data centers—and deploy them in appropriate environments for the best workload execution. The enterprise AI platform manages AI models throughout their lifecycle, automating the extraction of business insights and delivering AI-enhanced customer or business experiences across an organization.

4.3.3. Market Leaders in AI Platforms

Gartner's 2020 AI platforms MQ report assesses how well service providers fulfill enterprise requirements for implementing AI. The core analysis is based on clients' inputs, focusing on their needs for core AI support delivered on enterprise-grade AI platforms and corresponding services. The included providers represent those best equipped for supporting internal business operations or offering AI as a primary service to address various project needs involving supervised and unsupervised machine learning for organizations across diverse sectors.

Microsoft Azure IoT Central is a software-as-a-service (SaaS) solution designed to reduce the burden and accelerate the creation of IoT solutions. Users can connect devices securely to the cloud, monitor their performance, manage their lifecycle, set up rules and actions, and eventually analyze all the data generated. MicroStrategy offers an enterprise business intelligence platform that also has native integration with R and Python scripts, enabling quantitative analysts to build predictive models that generate future insights and then embed those results deeply into MicroStrategy reports. Together, partners connect the world through advanced, secure, and scalable low-code IoT solutions that allow builders to focus on solving their hardest connectivity challenges and getting their enterprise-connected devices to market rapidly at a predictable cost [5-7].

4.4. The Intersection of IoT and AI

The ability of IoT technologies to generate vast quantities of useful information from sensitive, embedded devices in an affordable way complements AI platforms, which are favourable for big data processing and analytics. At a basic level, IoT opens an additional and expansive data channel accessible to AI and other automation technologies. At a more involved level, intelligence can move closer to devices and edges by embedding artificial intelligence within the ecosystem of connected devices composing the Internet of Things.

It is common to deploy an intermediary device, such as a smart hub or gateway, providing edge computing and processing capabilities to enterprise-grade IoT deployments. Such edge devices support substantial processing and storage resources, an expert zone of specialisation that IoT has made even more accessible. The IoT-edge relation is bidirectional, given that IoT devices also supply the edge computer with raw data. Merging IoT systems with edge computing creates larger and more comprehensive machines equipped with data, processing, and actuation features specific for enterprise-grade use, capable of delivering substantial levels of intelligence, even in environments characterised by poor connectivity.

4.4.1. How IoT Enhances AI Capabilities

An enterprise-grade AI platform often benefits from hands-on experience with managing IoT and other connected devices. Every connected device, vending machine, ATM, retail

Fig 4 . 2 : Enterprise-Grade AI Platform for IoT Management

kiosk, connected car, or machine on the factory floor can provide sensors that provide additional information about the operation of the devices. Leveraging this information offers the opportunity to perform analysis on the actual usage of the device and

determine which parts need replacement or replenishment. An additional function is the ability to determine how connected devices are delivering results in applications such as credit card transactions or dispensing products. Using secrets management capabilities ensures that credit card data, banking information, or dispensing credentials are always protected, and if an issue occurs either through tampering or technical failure, being able to instantly revoke or update access credentials can be key to mitigating the risk associated with any large deployment.

Moreover, access to live telemetry from the connected devices in the field further enhances the real-time decisions it can make on behalf of the business. Incoming or outgoing message queues can easily be used to send the devices messages that acknowledge errors, or alert the operator if the transaction or dispense has been successful, or update the device operating parameters, such as temperature thresholds or inventory replenishment request parameters. The return path created through device connectivity offers an additional feedback loop that allows systems outside of the connected device ecosystem, such as supply chain, customer experience, or product development, to extract meaningful insights from the data collected and submitted by the device.

4.4.2. Data Collection and Analysis

A complementary process begins by considering events not originally noted among the objectives. Once AI platform objectives are well defined, scenario modeling identifies additional events associated with specific sensor types or actuators that can extend the main analysis. The attention mechanism focuses on these candidate events to track their appearance in the data, which is then re-examined whenever the mechanism concludes that an event deserves further scrutiny. Machine learning methods operating on a wide range of data also highlight additional events. Identified events gain full investigation, cataloging, and subsequent closure, meaning their potential is either applied within the project or allocated to the idle backlog in a prioritized fashion for later consideration.

The attention mechanism examines the continuous data stream from the Internet of Things layer to detect regular and exceptional events of interest. Detected events are matched against the AI platform's objectives to determine relevance. Events classified as relevant form an ephemeral knowledge base, extracted as needed from the original data trace and structured in machine-readable representations such as RDF graphs and OWL ontologies. Having all knowledge in one temporary structure allows the processing engine to associate distributions and compute summary statistics coherently for a particular set of AI objectives [1,3,5].

Real-time analytics differ markedly from summary statistics, especially when each objective associates data with a sampling fraction that has not yet closed. Shape-based time-series classification assigns stage labels to each data point, determining the state of the target complex system in time. These labels direct decision support processes to act accordingly.

4.4.3. Real-time Decision Making

Beyond expansion through multiple complementary data sources, the combination of IoT and AI also enables real-time decision-making by automating the flow of information between the two technologies. IoT devices naturally collect information on a cyclical schedule based on the polling period. Furthermore, certain types of devices, such as connected cameras, can even artificially extend the interval length of their data collection. Consider an on-premise surveillance camera; rather than constantly sending a video stream, it can instead process images on-device and generate a notification for human review when action is required. Based upon the continually growing AI capability on-device, ML components can be trained to distinguish between objects and alert only when a human needs to review and then decide to take action.

4.5. Architectural Considerations

It is obvious to any profitable business to develop the integration of Internet of Things and ISM devices into its architecture, contributing to more control and management of its implementation and less impact on its services. However, mistakes made in any organization have an impact on the Internet of Things and the management of Remote Locations. Companies have to complete the automation process by using Cloud Computing and Artificial Intelligence to support business decisions. These solutions in IoT applications with specific services and needs of local systems located in the field agree with Business Intelligence and control. Today, IoT lowers costs, tolerates risk, and increases efficiency. Moreover, business cost, value, and competitive positioning demonstrate innovation-quality service, from resource management to service delivery. Fields such as Smart City, Smart Building, Smart Home, Smart Factory, Smart Agriculture, etc., promote that mission [2,4,6].

The Internet of Things and Smart Cities concept has evolved rapidly thanks to advances in electronic devices, communications, mobile, and remote sensing technologies that together enable the development of smart and intelligent objects. Together, several technological areas integrate to form the smart opaque world: microelectronics and advanced sensors that shape the smart objects, wireless communication for the materialization of the network, the fusion and analysis of data, which has allowed the

use of Machine Learning Techniques, enabling a transition from a human-controlled world to an artificial intelligence-controlled one.

4.5.1. System Architecture for Integration

Integrating IoT and Connected Devices into Enterprise-Grade AI Platforms introduces a typical architecture for such a platform and shows how it can be extended to provide IoT device data. Enterprise systems and applications often reside in private datacenters or public cloud instances, so the example uses an external device gateway service that can communicate with devices deployed in other network topologies. Example scenarios include asset tracking for a global supply chain or real-time monitoring of equipment at customer sites worldwide. IoT-connected devices usually operate behind restrictive firewalls, on networks that prohibit inbound connections. Therefore, the gateway service must handle the device registration, provisioning, authentication, and authorization.

The architecture uses one of the leading enterprise platforms for deploying AI solutions at scale and in production. Its builder environment provides a complete set of tools for annotating, labeling, parsing, aggregating, and analyzing data streams from IoT-connected devices, including sensitive AI workloads for protecting intellectual property or implementing safety requirements. In the ground-truth use case, Chick-fil-A locations use the platform services to run real-time, AI-based monitoring of ordering lanes and kitchens [6-8]. The Google Cloud IoT integration should apply to other enterprise platforms with equivalent functionality.

4.5.2. Data Flow and Management

The data flows between connected devices and an enterprise-grade AI Platform can be described in a layered functional architecture. At the bottom layer, physical sensors located at the edge collect and measure data, such as GPS location. At the top layer, enterprise systems, including databases and Enterprise Resource Planning (ERP) systems, are located in the corporate office.

Typical use-case sensors do not operate at full capacity at all times because reporting and monitoring are interrupted by various disruptive events. The availability and quality of service requirements can be separated into two main categories: business continuity and business process monitoring. Business continuity requires that the sensors continue to operate during power and other infrastructure outages to mitigate overall risks to the enterprise. Business process monitoring requires that sensors monitor the underlying business processes and provide alerts when the business process channel capacity is affected.

Business Process Monitoring defines the logic of a sensor. Its purpose is to ensure the service quality of the whole pipeline of a business. Business Continuity ensures the continuous operation of the sensor during power and connection outages. Business Continuity also minimizes the traffic drop on the supervised pipeline. At the end of the reporting chain, corporate ERP or Core Business Systems supervise service quality at an enterprise-grade level, which defines the overall business process.

The data management strategy provides business process monitoring against the business continuity store data request, making it a ring-orbital support system. In case of a logistic support problem, an operational external system (e.g., for deploying and replenishing trucks and first responders) triggers a business continuity data storage request to the subsystem. At the beginning of the workflow, a business continuity store data request blocks the data transmission to map data onto the ring orbital current traffic situation.

4.5.3. Security Considerations

Businesses must recognize the potential security implications of making IoT data available to third parties. For example, when deploying IoT use cases across many parts of a factory, developers should consider the potential for the components to be used as entry points into an enterprise network by malicious actors. In an industrial control system, a breach can have permanent physical effects such as shutting down production processes or impairing equipment. In the context of Retail or Hospitality, a smart-payment system left vulnerable to attack could risk loss of customers' payment details, and put the company at risk of non-compliance with PCI DSS standards. Hosting sensor devices jointly with production machinery creates an additional surface area for potential attacks.

Businesses should therefore ensure that IoT data streams are adequately encrypted, while distributed payloads should be designed to protect endpoints, such as the processing of payment transactions. They should also consider the implications of sending IoT data over networks managed by third-party companies, especially when performing transactions or sharing operational business data.

4.6. Implementation Strategies

Fullwise has created a platform for deploying its proprietary general artificial intelligence agent and providing a marketplace for vendors offering other artificial intelligence agents. To incorporate data sourced from sensors, robots, and Internet of Things (IoT) devices, the system requires software containers capable of executing on a

broad range of devices and supporting all common operating systems. This compatibility ensures seamless integration of external data into the Fullwise platform.

The necessity for widespread software container support arises from Fullwise's centralized AI service model. The platform's primary AI service executes on Fullwise servers and engages in dialogue with external AI agents and customers. Maintaining a constant connection to external data through communication with these AI agents demands the capability to collect data from any and all sensors, robots, or IoT devices.

4.6.1. Step-by-Step Integration Process

The steady progress toward the implementation of smart environments based on the Internet of Things is having a direct impact on processes surrounding the development of enterprise-grade AI platforms and the way the underlying data is consumed.

Fig 4 . 3 : IoT's Impact on Enterprise AI Platforms and Data Consumption

Enterprises can ascertain information generated in all types of locations—whether inside or outside of company premises; on public infrastructures; on land, sea, or air transportation routes—even if such information is not generated by enterprise-grade assets[5,7,9]. To do so, the use of IoT services and platforms becomes necessary. However, enterprises do not usually build IoT capabilities internally; instead, they

employ either IoT platforms or IoT communication services offered by third parties. Some of the most widely used IoT communication services are Sigfox, LoRAWAN, IEEE EC-GSM-IoT, NB-IoT, LTE-M, and Ingenu.

Similarly, third-party IoT platforms are also available for adding XAI data consumption capabilities in the Cloud, gathering data from several archaeological sites. The data in these cases is supplied by several dedicated local authorities, such as the management and research business units of the archaeological sites of Alyki and Tithorea in Greece. Similar data from an IoT application scenario for protecting a historical site has been gathered at the Iklaina Mykenai Historical Site in Greece. The corresponding data is then consumed by a dedicated XAI application, offering XAI functions for solving a variety of cross-business use cases.

4.6.2. Best Practices

Negotiating connectivity sessions for a telematics-capable vehicle requires offering the lowest cost. Currently, AT&T charges $15 for a six-month data plan, and T-Mobile costs $10–$15 each month. Based on data usage profiles collected during initial trials, it may be feasible to select a personal hotspot or other connectivity mechanisms. To verify effectiveness, an

OCPP test scenario verifies the implementation of the Open Charge Point Protocol v2.0.1. The cloud charging platform acts as the main backend system of record. The Spotware Enterprise software is tested in a distributed fashion to verify interoperability among components and telematics-focused charging platforms communicating with roving corporate charging stations. The Enterprise software is offered as a hosted, cloud-service platform.

4.6.3. Common Pitfalls to Avoid

The integration of IoT technologies into an AI platform is not without potential issues. Connectivity is usually unreliable; a platform that assumes 100% connectivity wouldn't be fit for purpose. Some sites suffer from poor or even absent mobile coverage, and company Wi-Fi can be patchy at best. While an IoT platform should be location-aware to optimise traffic, mobile data costs can escalate dramatically if it assumes connectivity is available. Moreover, a shared supporting infrastructure constitutes a shared risk: a system failure or cyber-attack could affect thousands of sites. It is crucial to apply risk-mitigation strategies to minimise potential impact.

IoT also generates large amounts of data, especially when dealing with streams from connected machines. Ineffective categorization of data or overlooking strategies for

identifying and prioritising information can overwhelm the central engine, causing delays—and possibly downtime—in analysing other, non-IoT inputs. Given the severe consequences of such delays, it is essential to ensure that data loads remain within manageable and affordable limits.

4.7. Future Trends

A wave of new devices is ready to hit the market in the coming months, including refrigerators from Samsung with computers inside them, cameras from companies like Belkin and ConnectedIO that can make sense of your home and its security through the network, and some that can detect touch like Light Blue Optics. With wearables, the sensor type, considering contextual information, is also in this category. What makes this category distinctive is that these devices are no longer limited to being operated by a person; they can be connected to the Internet, one of the key defining elements of the Internet of Things concept.

One of the first Internet-connected electronic devices was the Coca-Cola vending machine at the Carnegie Mellon University Computer Science Department. Made in 1982, it could report its inventory and the temperature of the drinks to the ARPANET. The acronym was coined in 1999 by Kevin Ashton, and since then, dedicated researchers have been creating networks based on the Internet Protocol (IP) concept. The networking of smart devices is gaining more attention, and the Internet of Things discussion is already the center of attention for various Analyst firms, as well as industry events. The industry is also beginning to respond to the challenge of putting in place an infrastructure for supporting and managing this large and growing group of devices. Major service providers are at the table, including IBM, AWS, Microsoft, and Google. When viewed through the lens of a platform, the connection of any device to an artificial intelligence system can be categorized as one or more of the eight use cases described earlier.

4.7.1. Emerging Technologies in IoT and AI

Key to any discussion of emerging technologies is the term itself, yet its essence largely depends on the context. For example, most agree that an emerging technology generally lacks a long-standing tradition or extensive use but shows promise for long-term economic or societal impact. In the context of the Internet of Things (IoT), therefore, several subareas or related categories may also be considered emerging technologies, such as smart cities, connected vehicles, smart homes and appliances, connected health, and intelligent industrial machinery.

In addition, many other emerging technologies are being incorporated in the IoT ecosystem, including artificial intelligence (AI), big data and analytics, edge computing, and blockchain. Within AI, perhaps the most notable subareas are machine learning (ML) and deep learning (DL), both of which are gaining rapid acceptance within the business world. As organizations increase their use of AI to develop sophisticated enterprise applications, they rely more on a growing ecosystem of AI platforms and tools to assist in these efforts. Recent Gartner research highlights how the rapid increase in the use of AI is driving the need for a complex set of AI platforms.

4.7.2. Predictions for Market Evolution

Researchers and analysts debate when the smart systems marketplace will take off, determining the point in time when early adopters break away from the early majority and the market evolves rapidly. McKinsey and Company, with an implementation forecast of only four years, is among the most optimistic; IDC projects a timeframe of ten years[4,6,10]. The period between 2015 and 2020 is likely to see the emergence of the first connected-systems communities, a critical milestone in the marketplace development process that will indicate genuine customer commitment to and investment in large-scale deployments.

A McKinsey survey finds a majority of respondents viewing the emerging market for connected products as the next high-growth area, with their companies as leaders rather than followers in its development. Nevertheless, McKinsey's respondents identify questions in three categories as requiring answers: strategy and planning; buying and selling; operations and production. Strategic considerations include ecosystem design and development; product-level policy and rule base design; product architecture; big data analytic techniques; risk management and policy. Operational issues concern advanced underwriting and pricing; weighting model design; automated claims processing; and fraud analytics. Cash management, working capital projections, customer risk assessment, trade finance, supply chain monitoring, and audit are also cited.

4.8. Conclusion

AI at LLM scale is widely recognised as a foundational element of a broader, much more ambitious future state for the digital economy. While there is still much to be done, current LLMs can perform many complex tasks at or above the level of skilled people. Other aspects of that future state, including seamlessly augmented individuals and organisations using information, intelligence, and technology to successfully execute decision–making and planning at ever-increasing levels of complexity, are less well

recognised and understood. Achieving those future aspirations will require the integration of large-scale artificial intelligence together with all elements of information and technology environments, and the transformation of planning and decision-making processes that continue to execute the functions and activities of daily life. The following list identifies some of the features and capabilities important to a future state, and the level of sophistication and complexity it should be able to support: • Coping with the increased complexity of life and enterprise afforded by services such as AI at LLM scale that can readily operate in a broad set of domains, more generally. • Responding to the prevailing future needs of organisations and people – will those needs be easily understood by society and businesses, or will they also need analysing with the kind of introspective analytic capabilities of strong AI? • People and organisations working together as seamlessly joined units, each bringing that part of the joint capability that is best suited for any part of the action or activity, on the same intellectual plane. • Individuals working across several different organisations, both within and beyond society and nation-state structures, joined temporarily by specific decision-making or skill sets to tackle focused tasks.

Fig 4 . 4 : LLM Scale AI: Bridging Current Recognition & Future Aspiration

Many of these characteristics and considerations are outside the scope of AI—yet integration remains critical. Delivering these services requires smart IoT networks and cloud infrastructure working together to collect, store, and prepare data for seamless utilisation by LLM services. In addition, the IoT infrastructure must incorporate functionalities such as device management, access control, encryption, key and certificate management, data transfer and streaming, event processing and rule definition, and service monitoring, all of which support ongoing operation of smart IoT devices. Other required features include data ingestion and exchange, user and account management, mechanism-driven decision-making, and prediction capabilities. Relying on managed commercial services satisfies the need for greater sophistication, lower cost,

resource isolation, enhanced security, improved resilience, and better service-level agreements.

4.8.1. Key Takeaways and Future Directions

The success of AI as a venture capital sweet spot is due, in large part, to advances in enterprise-grade AI—AI platforms built to support a broad range of users across an entire organization rather than specialized niches. Platforms are what allow non-technical business users to extract useful intelligence from data without the help of data professionals, who remain perpetually overwhelmed by demand. The most popular platforms, such as Salesforce's AI-powered Einstein and Oracle's Autonomous Database, are being designed for use by business analysts and everyday business users.

Yet there is a crucial use case for which enterprise AI platforms have not been built: data "in the wild." IoT data is being produced in droves, as sensor-laden products and connected systems spread into every industry and as big cities begin to harness the power of technology to tackle their daunting congestion and pollution problems—yet most IoT implementations require machine learning experts, not average analysts. The world now demands AI that can support the use of connected devices and IoT data on an enterprise scale.

References

[1] Zhang J, Tao D. (2020). Empowering Things with Intelligence: A Survey of the Progress, Challenges, and Opportunities in Artificial Intelligence of Things. arXiv preprint.

[2] Pallav Kumar Kaulwar. (2025). Leveraging AI, ML, and Gen AI in Automotive and Financial Services: Data-Driven Approaches to Insurance, Payments, Identity Protection, and Sustainable Innovation. Journal of Information Systems Engineering and Management, 10(36s), 1118–1136.

[3] Siam S I, Ahn H, Liu L, et al. (2024). Artificial Intelligence of Things: A Survey. arXiv preprint.

[4] Munnangi, A. S. M., Nayeem, S. M., Koppolu, P., & Munnangi, S. R. (2025). Experimental and molecular dynamics study of molecular interactions in γ-butyrolactone–dimethyl formamide systems with machine learning based density predictions. The Journal of Chemical Thermodynamics, 107545.

[5] Panduman Y F, Funabiki N, Fajrianti E D, Fang S, Sukaridhoto S. (2024). A Survey of AI Techniques in IoT Applications with Use Case Investigations in the Smart Environmental Monitoring and Analytics in Real-Time IoT Platform. Information, 15(3):153

[6] AI-Based Financial Advisory Systems: Revolutionizing Personalized Investment Strategies. (2021). International Journal of Engineering and Computer Science, 10(12).

[7] Radanliev P, De Roure D, Van Kleek M, Santos O, Ani U. (2019). Artificial Intelligence in Cyber Physical Systems. arXiv preprint.

[8] Kishore Challa. (2025). AI and Cloud-Driven Transformation in Finance, Insurance, and the Automotive Ecosystem: A Multi-Sectoral Framework for Credit Risk, Mobility Services, and Consumer Protection. Journal of Information Systems Engineering and Management, 10(36s), 1084–1102. https://doi.org/10.52783/jisem.v10i36s.6706

[9] Raja P, Kumar S, Yadav D S, Singh T. (2023). Integrating IoT and AI: Enhancing System Efficiency and User Experience. International Journal of Information Technology & Computer Engineering, 26(39):50.

[10] IT Integration and Cloud-Based Analytics for Managing Unclaimed Property and Public Revenue. (2025). MSW Management Journal, 34(2), 1228-1248.