Assessment 2: Internet of Things (IoT) & Artificial Intelligence (AI)

Watson Ndethi

2025-02-23

Abstract

As an IoT Architect Engineer for ThingX, an IoT Solutions company, and as a Lead AI Developer for IntelligentX, an AI-driven startup I make recommendations for both business to thrive in the age of AI and IoT.

1 Exercise 1: Internet of Things (IoT)

1.1 Introduction

With possibly billions of devices interconnected already(cite Gartner article) and many more expected in the future, the role of the IOT Architect will continue to become ever more indispensable. In this assignment for ThingX, a formidable player in the home IoT space, the architect seeks to point out the challenges inherent in IoT rollout,make a case for onboarding IoT Data Analysts and attempt a high-level AI explainer targeted at management - specifically highlighting the different kinds of AI and their respective use cases.

1.2 Task 1: IoT Implementation Challenges

1.2.1 Security Risks

Inherent in their minimalist design(meant to lower energy consumption), IoT devices will often suffer from hardware with limited capabilities, unable to withstand the rigors of modern day cyberattacks. Coupled with a laxity (mostly from deployers) in securing IoT environments using high complexity passwords and leaving defaults in place, these devices become easy entry points for malicious cybercriminals looking to move exploit deeper into corporate networks [Fortinet (n.d.)].

1.2.2 Interoperability Challenges

The ability of IoT devices to work together and exchange information(interoperability) could be considered one of the defining characteristics of the technology. However, with different manufacturers individually employing a mix of varying and distinctly incompatible communication protocols e.g (WiFi, Bluetooth, Zigbee, Z-wave, LoraWAN, LwM2M) some proprietary and some open-source, integration across brands remains a major huddle. There have been recent attempts at standardizing these communication protocols for example through the Open Mobile Alliance (OMA) [O. M. Alliance (n.d.)] and Matter [C. S. Alliance (n.d.)] , with reputable bodies like IETF and IEEE leading parallel standard development efforts (hopefully this will not result in further fragmentation but coalesce into an agreeable regulatory framework)

1.2.3 Scalability Limitations

Often IoT devices will be distributed across vast geographical areas - some of these quite remote and outside coverage of connectivity, this makes artichecture considerations orders of magnitude more complex than in traditional network architectures. For example a smart camera part of a system that tallies no. of visitors to a remote dam in Somaliland, needs to connect to a GSM network to transmit daily tallies to a cloud hosted endpoint, but often signal at the dam is inconsistent leading to discrepancies in reporting.

1.3 Task 2: Making a case for IoT Data Analyst Role

1.3.1 IoT Data Analyst Role - Bridging Data and Decisions

IOT devices produce stagggering amounts of data ,with estimates of total data volume of connected devices in 2025 [Statista (2021)] expected to reach close to 80 ZBs. This sheer raw volume can be overwhelming for upper management, therein lies the opportunity for ThingX to hire IoT Data Analysts who having internalized ThingX' organisational goals can then perform data cleaning, pre-processing on the raw stream of data in readiness to identify patterns and trends that upper management can then act on. They ideally would sit between the data and the decision makers , feeding the latter actionable insights that ThingX can implement to reduce costs or improve revenue. An example of this would be by getting insights on the life of a battery in a solar powered security light, ThingX IoT Analysts can use predictive maintenance to inform engineers to regulate discharge cycles accordingly effectively extending the life of the said battery and thus lowering long-term maintenance costs. On the revenue front, the IoT Data Analysts having recognized a concerning rise in CO2 concentration levels in a certain neighhbourhood through one of the smart door bells that also reads weather info , ThingX can act pragmatically spinning up a new air purifier product targeted at residents of the area - a likely boon for revenue. In conclusion as is evident through the two examples, the centrality of the role of the IoT Data Analyst is unquestionable.

1.4 Task 3: The Categories of AI - Broadly Speaking

To comprehensively understand the various capabilities of Artificial Intelligence (AI) it is imperative to classify it into the below broad categories

1.5 AI Types and Applications

1.5.1 Narrow AI (Weak AI)

This would refer to AI that has been trained to perform a single task or narrow task. It excels in a single set of abilities. An example of an implementation of Narrow AI is virtual assistants like Amazon's Alexa and Apple's Siri. These perform not much else than letting the user control them and connected devices via voice. OpenAI's ChatGPT would be considered another surprising example of Narrow AI, as IBM puts it in this article [IBM (2023)]. Generative AI, that concernts itself with conjuring up new artifacts given some input, would also be considered a subset of narrow AI.

1.5.2 Artificial General Intelligence (AGI) (Strong AI)

AGI refers to machine intelligence that can mimic the cognitive abilities of a human brain [Google (2023)], uses existing knowledge to accomplish novel task in varying contexts independent of training of underlying models [IBM (2023)]. While in recent times, there has been talk of the feasibility of AGI [Altman (2023)], Artificial General Intelligence (AGI) remains largely hypothetical and theoretical.

1.5.3 Super AI

Also known as Artificial Super Intelligence (ASI) , this refers to AI that supercedes the cognitive abilities of human beings. This type of AI at present remains largely theoretical. A first step towards realizing ASI would be AGI.

1.5.4 IoT-AI

A Narrow AI implementation, leveraging a rule-based algorithm that acts on pre-defined business rules would be handy for IOT-AI integration. For example , ring the alarm if the motion sensor is triggered after midnight. On the other hand Generative AI can be used to write a comprehensive report to upper management given an IoT devices' sensor data, leveraging on this new found AI ability to make sense of otherwise unintelligible stream of ones and zeros. As we near AGI, AI will be able to act on patterns of data via Agentic AI, a new paradigm promising impressive levels of machine autonomy [Today (2023)].

1.6 Recommendations for ThingX

In light of the challenges and opportunities discussed so far regarding the IoT and AI space, ThingX would be well served to adopt three-pronged approach to bolster its position as a formidable player in the IoT domain:

1.6.1 Security-First Focus

Adopt a culture of security by putting in place and enforcing an IoT Security Policy which amongst other regulations, mandates regular audits , pen testing of edge IoT devices, prohibits manufacturer default credentials and employs AI for advanced real-time threat detection possibly via a sophisticated SIEM tool

1.6.2 Standardize for Max Interoperability

Rather than trying to support every protocol, standardizing on a single protocol like Matter for new products while only investing in other protocols to support backward compatibility with older devices, this will reduce production complexity moving forward while still supporting older devices. Building on Matter would allow greater functionality and if marketed as such could encourage upgrades to newer devices

1.6.3 Dedicated Data Analytics Team

While in this age of AI, it might be tempting to deploy an AI-powered analytics platform instead of hiring a team of human analysts, ThingX would be ill-advised to sever the human element as human analysts would still outshine AI in articulating business cases to upper management [Van & Colleagues (2021)]. That said however analysts who use AI would be better off than those that don't.

2 Exercise 2: Artificial Intelligence (AI)

2.1 Introduction

AI has brought the acronym soup to a nice simmer with the meanings of the abbreviations AI, ML and DL stumping even the most tech savvy of us. In the next session we try to demystify these often confusing terms.

2.2 Task 1: AI, ML, and DL Distinctions

2.2.1 Artificial Intelligence

Artificial Intelligence (AI) is a broadest term amongst the three referring to any technology that allows computers to imitate human intelligence and behaviour. A thermostat that adjusts temperature depending on time of day using rule-based algorithms would be a good example. Notice while this is by definition AI, it does not necessarily involve much complexity.

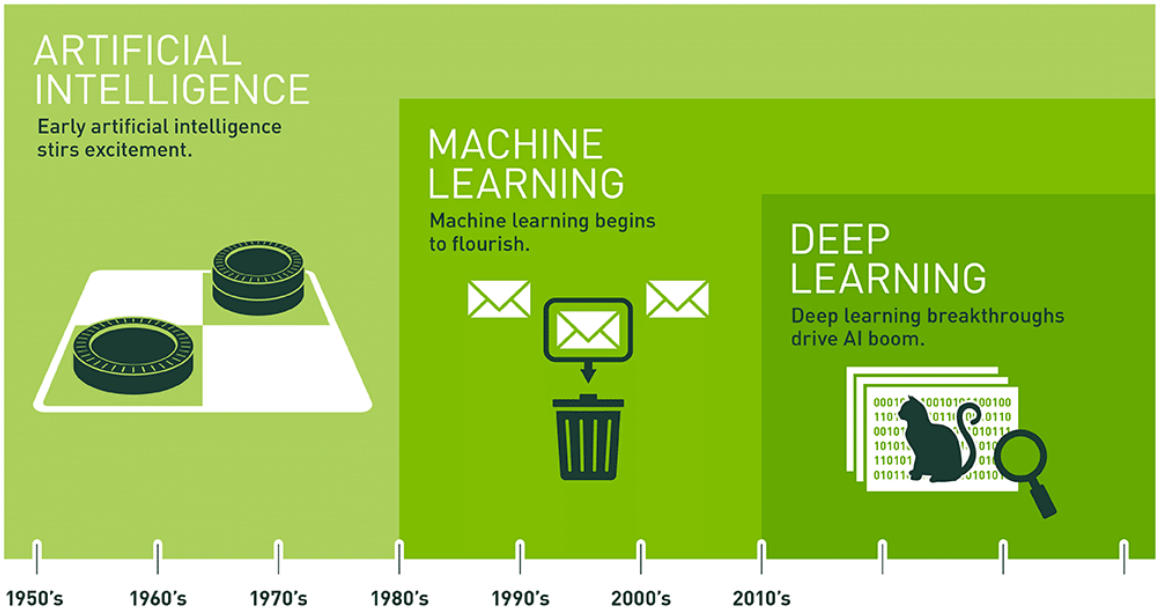
2.2.2 Machine Learning

Machine Learning (ML) represents a subset of Artificial Intelligence (AI) that can learn from data without explicit programming [Corporation (n.d.)]. A commmon usecase of ML is intelligent recommendations used by online retailers for personalized marketing. Shopper's purchase history is used as data that feeds the ML models resulting in personalized recommendations - supporting the upselling ecosystem.

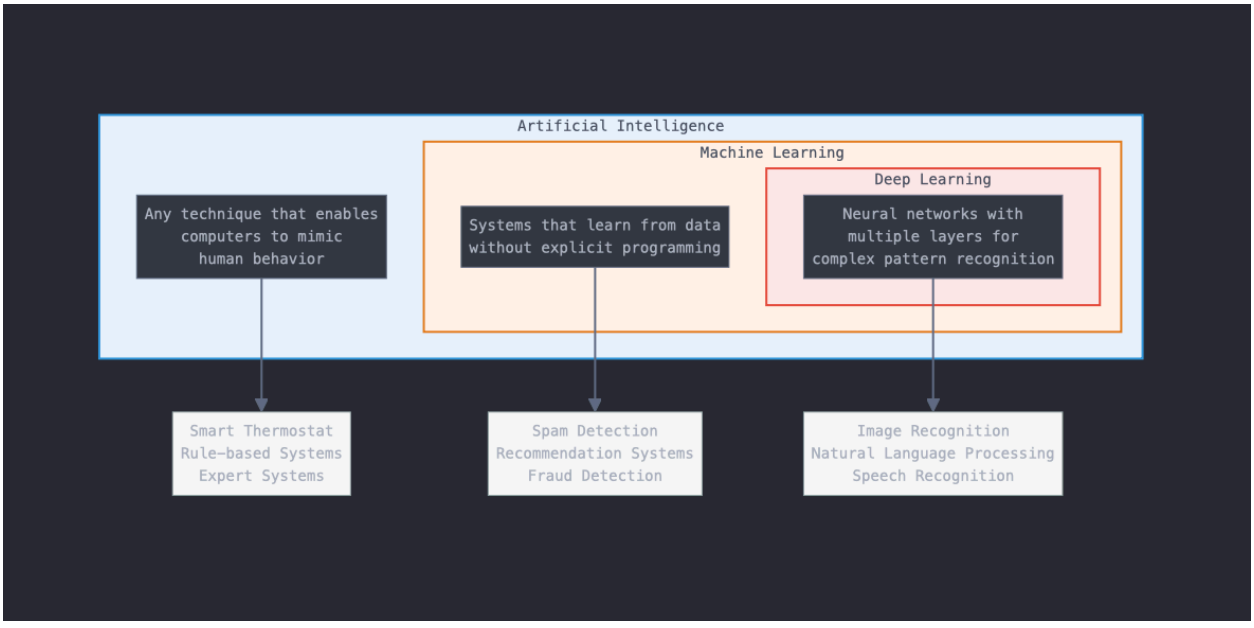
2.2.3 Deep Learning

Deep Learning (DL) is a subset of Machine Learning (ML) wherein DL algorithms can automatically learn from data (e.g., images, video, and text) without explicit human domain knowledge. The term "Deep" refers to the layered architecture used to identify complex patterns. Common use cases include speech recognition, object detection, and language translation [Corporation (n.d.)]. DL is the pivotal technology powering self-driving cars and conversational AI.

2.2.4 AI vs. ML vs. DL – An Illustration



Since an early flush of optimism in the 1950s, smaller subsets of artificial intelligence – first machine learning, then deep learning, a subset of machine learning – have created ever larger disruptions.



2.3 Task 2: Machine Learning in IoT Security

2.3.1 Advantages

2.3.1.1 Enhanced Anomaly Detection Capabilities

By establishing a robust baseline of typical IoT activity, ML algorithms can quickly detect irregularities. Once a proper alerts pipeline is established, administrators receive timely notifications for fast action.

2.3.1.2 Predictive Maintenance Benefits

Leveraging historical data, ML models can forecast when operational failures are likely, enabling proactive maintenance that saves both equipment lifespan and costs [PTC (2023)].

2.3.2 Disadvantages

2.3.2.1 False Positives

Despite high accuracy, ML systems may sometimes flag normal events as suspicious due to inherent training biases [Smith & Doe (2024)].

2.3.2.2 Resource Requirements

Running ML workloads on the vast streams of IoT data demands significant compute and storage resources, resulting in substantial operational costs.

2.3.2.3 Adversarial Attacks

ML systems are vulnerable to cyberattacks; for example, data tampering during training can compromise model inference accuracy [University of California (2023)](https://cltc.berkeley.edu/aml/#:~:text=An%20adversarial%20atta

2.4 Task 3: Explainable AI (XAI)

2.4.1 XAI Overview

Explainable Artificial Intelligence (XAI) consists of processes and methods that enable human users to understand and trust AI outputs [IBM (n.d.)]. This transparency is essential in regulated sectors like healthcare and finance, where decision rationale is critical. For IntelligentX, implementing XAI would:

- Build trust with key stakeholders and customers.
- Ensure regulatory compliance, particularly for AI applications interfacing with banking systems (e.g., credit scoring).

2.4.2 Building Trust with XAI

Deploying XAI is crucial for IntelligentX's compliance framework; it will:

- Enhance transparency in AI-driven health applications, boosting trust among users and providers.
- Improve customer experience in AI-powered microlending apps by clarifying the credit approval process.
- Enable internal teams to mitigate model drift by proactively addressing deviations [IBM (n.d.)].

2.5 Recommendations for IntelligentX

2.5.1 Monitoring Priorities

2.5.1.1 Model Performance

Resource utilization - imperative to evaluate if use of compute is optimizal

2.5.1.2 Fairness and Bias

Need to manage fairness and scan algorithms and data for biases and manage them accordingly

2.5.1.3 User Experience

Consider user satisfaction and usage metrics

2.5.1.4 Security Monitoring

Audit access control and secure authentication practices

2.5.2 Implementation Framework

To effectively evaluate the above areas , IntelligentX should: - Establish a lean Responsible AI team (with one technical and one strategic resource) that sits between the devs and management, whose job will be to maintain general health of their models - Use automated observability tools to monitor resource utilization - Develop an AI Policy and Manifesto and in it clearly illustrate escalation protocols (for when biases/deviations occur)

References

Alliance, C. S. (n.d.). *Matter – the new smart home standard*. https://www.csa-iot.org/all-solutions/matter/

Alliance, O. M. (n.d.). *Open mobile alliance standards*. https://www.openmobilealliance.org/

Altman, S. (2023). *The future of AGI: An interview with sam altman*. https://www.example.com/sam-altman-agi

Corporation, N. (n.d.). *NVIDIA AI: Machine learning and deep learning*. https://www.nvidia.com/en-us/deep-learning-ai/

Fortinet. (n.d.). *Fortinet IoT security report 2023*. https://www.fortinet.com/blog

Google. (2023). *Google cloud platform: IoT and AI innovations*. https://cloud.google.com

IBM. (n.d.). *Explainable AI: Building trust and transparency*. https://www.ibm.com/thought-leadership/ai/explainable-ai

IBM. (2023). *IBM 2023: AI transforming industries*. https://www.ibm.com/ai

PTC. (2023). *Predictive maintenance in IoT*. https://www.ptc.com/en/predictive-maintenance

Smith, J., & Doe, J. (2024). False positives in machine learning security. *International Journal of Cybersecurity*, *12*(3), 45–67. https://doi.org/10.1234/ijc.2024.12345

Statista. (2021). *Statista: IoT industry - facts and figures*. https://www.statista.com/topics/2632/internet-of-things-iot

Today, I. W. (2023). *IoT world today: Evolution of the internet of things*. https://www.iotworldtoday.com

University of California, B. (2023). *Adversarial attacks on machine learning*. https://www.berkeley.edu/machine-learning/adversarial-attacks

Van, J., & Colleagues. (2021). *Trends in IoT integration with machine learning*. https://www.example.com/van2021