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?**)] 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

1.4.1 AI Types and Applications

- ## 1.5 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 [(**ibm2023?**)]. Generative AI, that concernts itself with conjuring up new artifacts given some input, would also be considered a subset of narrow AI.

- ## 1.6 Artificial General Intelligence (AGI) (Strong AI)

  AGI refers to machine intelligence that can mimic the cognitive abilities of a human brain [(**googlecloud?**)], uses existing knowledge to accomplish novel task in varying contexts independent of training of underlying models [(**ibm2023?**)]. While in recent times, there has been talk of the feasibility of AGI [Altman (2023)], Artificial General Intelligence (AGI) remains largely hypothetical and theoretical.

- ## 1.7 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.

1.7.1 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 intelligible 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 [(**iotworldtoday?**)].

1.8 Recommendations for ThingX

- Proposed IoT-AI integration model
- Implementation strategy
- Risk mitigation approach
- Expected benefits and ROI analysis

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: * ### 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 * ### Starndadize 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 * ### 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 [(**van2021?**)]. 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.

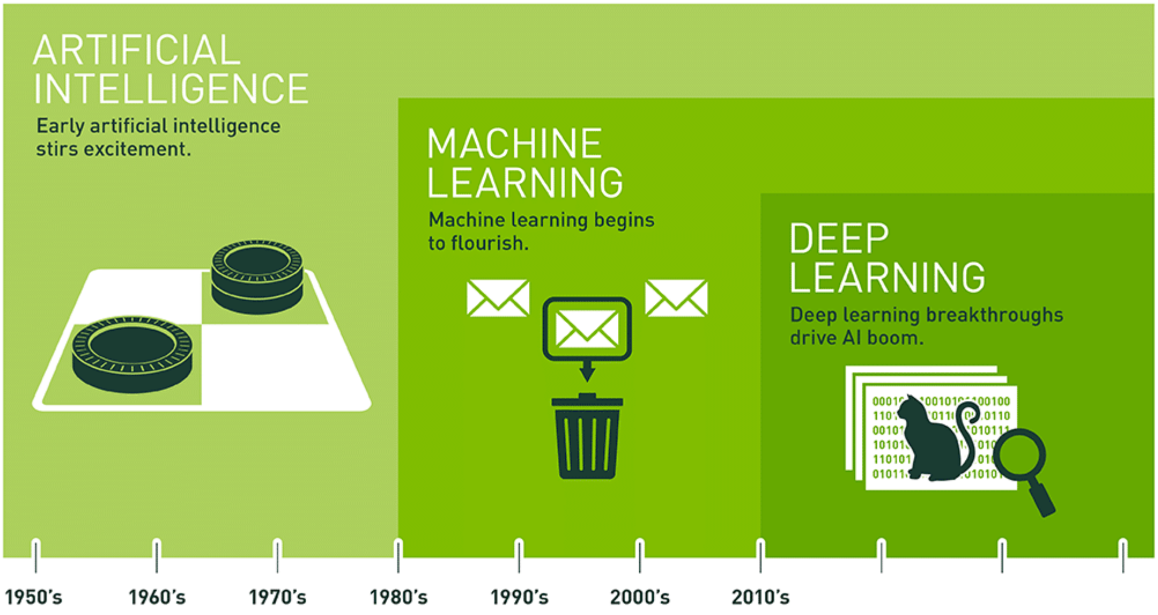
2.2.2 Machine Learning

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) but where DL algorithms can automatically learn from data such as images, video and text without the introduction of human domain knowledge. The term 'Deep' in DL represents the layers of algorithms used to identify patterns in data. Common usecases of DL 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 v. ML v. DL - An Aillustration


ARTIFICIAL INTELLIGENCE
Early artificial intelligence stirs excitement.
MACHINE LEARNING
Machine learning begins to flourish.
DEEP LEARNING
Deep learning breakthroughs drive AI boom.
1950's
1960's
1970's
1980's
1990's
2000's
2010's

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.

Figure 1: Figure 1: AI vs ML v DL

graph TD subgraph AIArtificial Intelligence A[Any technique that enablescomputers to mimichuman behavior] subgraph MLMachine Learning B[Systems that learn from datawithout explicit programming] subgraph DLDeep Learning C[Neural networks withmultiple layers forcomplex pattern recognition] end end end

```
style AI fill:#e6f3ff,stroke:#3498db,stroke-width:2px
style ML fill:#fff2e6,stroke:#e67e22,stroke-width:2px
style DL fill:#ffe6e6,stroke:#e74c3c,stroke-width:2px

%% Examples for each level
E1[Smart Thermostat<br/>Rule-based Systems<br/>Expert Systems]
E2[Spam Detection<br/>Recommendation Systems<br/>Fraud Detection]
E3[Image Recognition<br/>Natural Language Processing<br/>Speech Recognition]

%% Connect examples to their categories
A --> E1
B --> E2
C --> E3
```

```
%% Style for example boxes
style E1 fill:#f9f9f9,stroke:#95a5a6,stroke-width:1px
style E2 fill:#f9f9f9,stroke:#95a5a6,stroke-width:1px
style E3 fill:#f9f9f9,stroke:#95a5a6,stroke-width:1px
```

2.3 Task 2: Machine Learning in IoT Security

2.3.1 Advantages

-

2.4 Enhanced anomaly detection capabilities

Having learnt what comprises a normal baseline of IoT activity, ML algorithms can easily ,with speed and at scale detect irregularities and if a proper alerts pipeline has been set up send notices to the admin about said inconsistencies for quick action

-

2.5 Predictive maintenance benefits

By using historical data from IoT devices over time, we can predict when certain operational failures are most likely to occur and plan for maintenance accordingly, saving the equipment and money (PTC, 2023).

2.5.1 Disadvantages

-

2.6 False Positives

While largely accurate, it is inevitable that ML may flag some events as suspicious while in fact being normal due to biases inherent in training data (Smith & Doe, 2024)

-

2.7 Resource Requirements

Training and running ML workloads on the magnitude of data that IoT devices produce requires significant compute and storage resources and the inherent costs are non-trivial.

-

2.8 Adversarial Attacks

ML systems themselves are not immune to sophisticated cyberattacks; for example, introducing data inaccuracies during training contaminates the inference results University of California (2023).

2.9 Task 3: Explainable AI (XAI)

2.9.1 XAI Overview

Explainable Artificial Intelligence (XAI) is a set of processes and methods that allows human users to understand and trust results and outputs created by AI (IBM, n.d.). It is especially crucial in regulated industries like medicine and finance, where the transparency of decision-making is paramount. For IntelligentX, implementing XAI would: * Build trust with key stakeholders particularly their customers * Seeing that some of

IntelligentX' AI-powered applications interface directly with banking apps, by implementing XAI best practices, IntelligentX ensures regulatory compliance with banking policy landscape that demands XAI especially for credit scoring applications

2.9.2 IntelligentX building Trust with XAI

Considering IntelligentX develops some AI solutions in the Healthcare and Finance domains, deploying XAI is core to its compliance pillar. Explainable AI will: * Improve transparency in decision making of AI-powered health apps, improving its trust by users and health providers alike * Boost Customer Experience in its AI powered microlending app by laying bare the credit approval process while ensuring compliance with credit regulations on traceability in decision making on user creditworthiness * For the internal dev teams, model drift mitigation and model drift management achievable through XAI (IBM, n.d.), will allow developers to get ahead of model deviations and mitigate the resultant risks accordingly

2.10 Recommendations for IntelligentX

2.10.1 Monitoring Priorities

- ## 2.11 Model Performance

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

- ## 2.12 Fairness and Bias

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

- ## 2.13 User Experience

  Consider user satisfaction and usage metrics

- ## 2.14 Security Monitoring

  Audit access control and secure authentication practices

2.14.1 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

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

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