WSO2CON 2024

Unlocking Value with AI



Srinath Perera
Chief Architect
WSO2



We do not care for AI, rather value it creates!!
The outcome depend more on leverage points than intensity of force.



AI, what changed?

- LLM
  - Build models with little data and little training
  - LLM enables extracting more info; even older ML models can now have more data
  - LLMs can interpret the outputs of other models
- New Toolset
  - Chat APIs
  - RAG
  - Embeddings
  - Supervised Models
  - Audio, video processing





Use Cases: Quality Control

- Apparel Manufacturing Quality control
  - Hold the fabric against a board that has measurements
  - Show green /red if passed failed
  - Reducing the defects has a huge impact on the bottom line
  - The process improved customer confidence

What is Digital Transformation looked like?

- Internal
  - Fast Delivery and continuous improvements (lead time to a change, growth hacking)
  - Data-driven decisions - (e.g., Predictive maintenance, planning)
  - Connecting disconnected parts - programmable business with APIs, interoperability
  - Automation (e.g. Robotic Process Automation)
- External
  - Rethink UX using new tech (e.g., Uber, Digital banks) - focus on customer journey,
  - Solve a significant bottleneck or add value using new tech (e.g., AI, blockchain, VR)
  - Significant uplift in customer support - AI, Multi-channel customer support, keep context, be responsive, proactive,
  - New revenue streams/business models - e.g., sell data, new APIs



Use Cases: Make Product/Website Seamless

- Personalization
- Recommendations
- Documentation Chatbot
- Contextual chat at any point
- Suggest next steps based on where you are
- Educational suggestions and explanations
- Make giving input easier
- Auto correction, filling
- Forecasts, Alerts, suggestions, interventions
- Adaptive user experiences - make UI adept to the user

Use Cases: Customer Support

- Product Support
  - AI as first-level support / Troubleshooting help
  - Need to go past negative impressions
  - Warnings when things could go wrong
  - E.g., Klarana – ⅔ customer service chats handled , and Coda payments use AI to handle simple queries and filter SPAM
- Improve Support Ops
  - use it in the back office to help the team
  - Suggestions - proactive
  - Keep the context, summarize
  - Flags tickets that might be escalated
- Churn forecast – focus your efforts





Use Cases: Digital Twin

- Virtual version of physical things
  - NASA uses physical/ digital twins
  - A twin is a model of a specific aircraft, car, etc, with actual data, forest, farms, vehicles, ppl, etc
  - Sometimes, predictive physics-based models are used
- Use cases
  - Respond to surprises in automated warehouses, factories
  - Manufacturing residence with twins
  - Simulate a faster checkout experience
  - What if I change this?



Use Cases: Remove Friction

- Examples
  - Apple FaceID
  - Guess and provide updates the user wants right away - e.g., lost luggage
  - Configure themes - point to a website with the theme
  - Remove the need for configs - figure out the right value with AI
  - Passport clearance by just walking through
  - Scan the passport to check

Use Cases: Secure Your Systems

- Biometric Authentication, e.g., facial, fingerprint, and voice recognition
- Behavioral Analytics leverages user behaviors such as login patterns, typing speed, and usual IP addresses to effectively detect potential attackers.
- Risk-Based Authentication: assess the risk level through factors like user location, device security status, and the actions sensitivity to trigger MFA.
- Fraud Detection for Access Requests: The above is used to identify fraud.
- (more examples in CIAM sessions)



How to make the AI Happen?

Is there a non AI Solution?

- My first reaction when someone talks about a AI use case is to think about another way to solve the problem.
- Why?
  - AI solutions are almost always more expensive
  - More complex
  - Require more effort



This style of thinking can save you a lot of $$ and time - e.g. Empty box, Cao Chang Weigh the elephant.

Checklist

- Is value clear?
- Can we solve it without AI?
- How do you know it is working? You need test data.
- Who owns the data/ model? Are there privacy/ copyright concerns of that data/model?
- Do we know how to use the outcome? Have we thought through how to integrate it with existing processes? What actions can we take? How to implement those actions
- What are the risks associated with wrong forecasts and those actions?
- Who will operate it?



Churn as a Motivating Example

- Value - a lot of recurring revenue saved, also CAC
- Can we solve it without AI? Can you beat the current model
- How do you know it is working? You need test data - likely you have
- Who owns the data/ model? Are there privacy/ copyright concerns of that data/model? Terms need to cover this.
- What actions can we take?
- Risks - Small
- Who will operate it?



Digging into Risk

- Risks
  - Bias
  - Forecasts intruding on privacy
  - Data Ownership
  - What happens to the other 1%
- Common safe Categories
  - The risk of a wrong forecast is small (recommendations)
  - Humans can select proper responses (e.g., Google)
  - The outcome of a mistake is critical, but there is enough data to get high-level accuracy (e.g., Self-driving)



Making the model Real

- Build the model to verify the accuracy
- Deliver the model to a limited audience - fine tune (within the org)
- Fine-tune their actions
- Update with new data, test, and roll-out
- Continuous tests
- Monitor and look for drift and surprises



Baby Sit Your Models



- Running a model is like having a fox as a pet; you need to keep counting your chicken
- We do not fully understand how models work
- We need to verify and release them gradually
- Humans make more mistakes - but
  - Each makes different mistakes
  - Often, we can see those decisions
  - With AI, it is the same mistake under the radar
- They can go out of control; we need to have guardrails

Conclusion

- It is about the value
- Are their non-AI solutions? yes, use them
- What can we do with the results?
- What are the risks associated with actions?
- Babysit your models and manage risks.



Question Time!



Risks

- Privacy
- result verification
- data quality and availability
- integration with existing systems
- costs and ROI concerns
- ethical considerations
- , bias concerns,
- Scalability
- maintenance



Thank You!