Cyber Security for Digitalized Grids

Cyber Security with Explainable Artificial Intelligence

Speaker : *Aswini Vadapalli, Associate Product Manager, Fluentgrid*

Overview

Evolution of Grids

The energy sector is evolving rapidly with modernization and rapid transformations of traditional electric grids into smart grids.

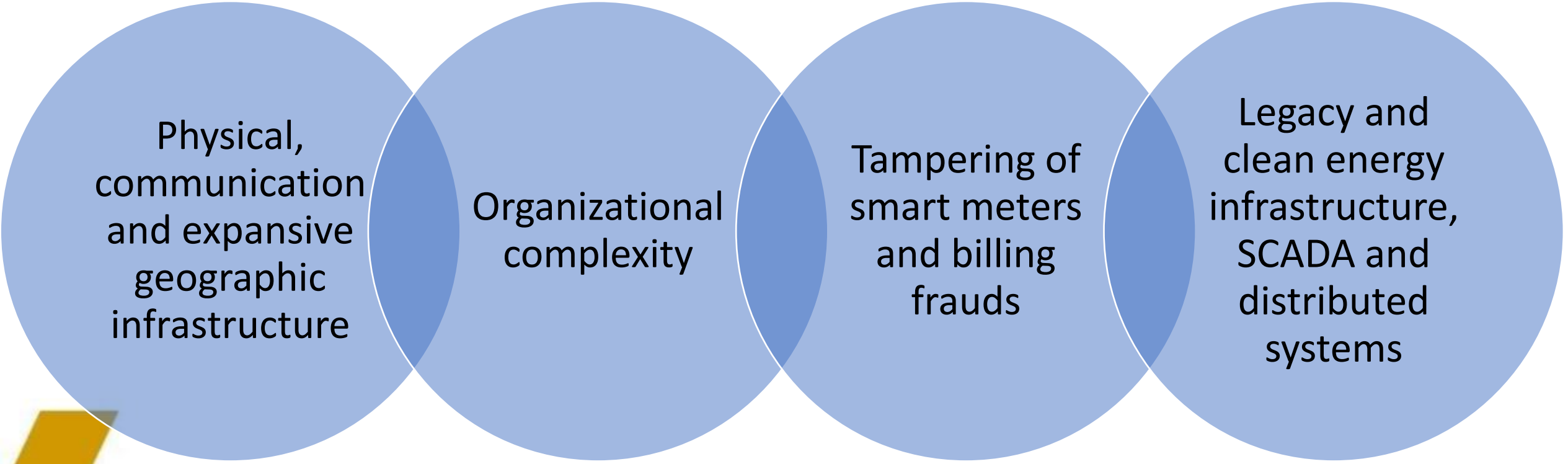
Technological Advancements and Digitalization

E-Vehicles, smart metering, distributed renewable energy, and competitive retail energy markets are ushering in a slew of technological advancements that are one or the other way inter-connected and use digital communications.

Brief Background

Topics	
Cybersecurity	▪ Cybersecurity in Energy Sectors ▪ Vulnerabilities ▪ Current Standards and Guidelines
XAI and Guidelines for implementations of XAI	▪ What is XAI? ▪ Why XAI? ▪ Brief comparison of XAI with other AI Techniques ▪ Implementation of XAI with Data Driven Model
Various scenarios and Challenges	▪ Scenarios in energy sectors ▪ Challenges with XAI

Cyber Security and Vulnerabilities



Standards and Classification of Cyber Attacks

Current Standards and Guidelines	• ISO/IEC 27001, ISO/ IEC 27019, ISO/IEC 61508
Classification of Cyber Attacks	• Component • Topology • Protocol
Consequences of Cyber Attacks	• Damage to Equipments • Loss of Service • Data Breach

Cyber Security using XAI

What is XAI?

Reason for choosing XAI

Comparison of XAI and other AI techniques

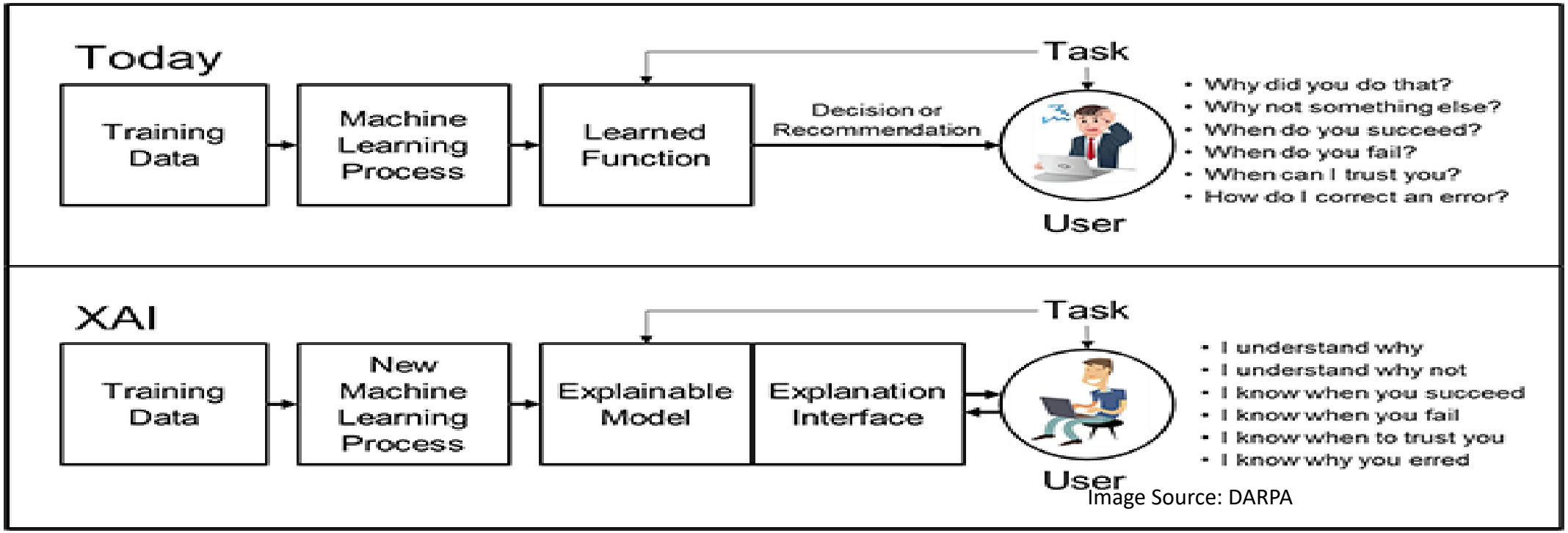


Image Source: DARPA

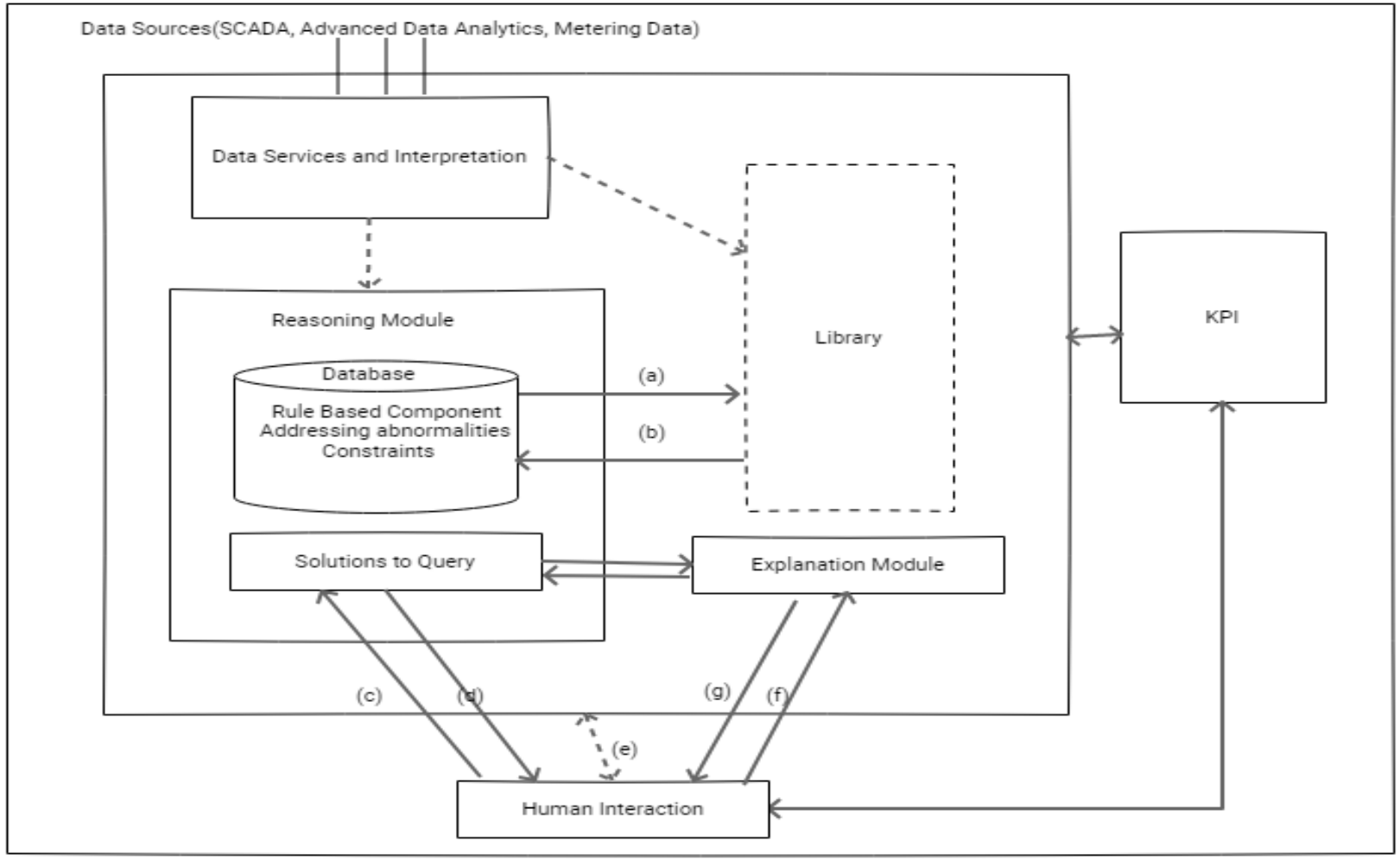
Implementation of XAI

Here, Data Driven Model is considered for the implementation of XAI

- Data Service and Interpretation
- Reasoning Module
- Explainability
- Human Interaction

There are other models/tools/methods like SHAP,LIME

Data – Driven Model



Data – Driven Model

Data Services and Interpretation - Gathering Data, Streamlining and Cleaning Data.

Library - library of services, to understand the executed tasks

Reasoning Module – a)*Rule-based component b) Constraints c) Addressing abnormalities*

Explainability- Crucial for security systems to adapt to constantly changing environments.

Human Interaction- Transparency , understandability, interaction and feedback from the system.

KPI- Establishing a set of KPIs to generate relevant metrics

Various Scenarios

1. **Smart Grids:**

2. **Customer Information**
3. **EVs and EV-Infrastructure**

Challenges of XAI

- *Interference of algorithms*
- *Dynamic decision data*
- *Lack of expertise*
- *Nature of the problems*

Conclusion

- Explainable Artificial Intelligence is rapidly growing in recent years, but there is very limited research on “Cybersecurity in Energy Sector using XAI”.

- Further research can be made based on performance, and trustworthiness of the system.

Thank You

For discussions/suggestions/queries email: www.indiasmartgrid.org
www.isgw.in
Links/References (If any)

India Smart Grid Forum
CBIP Building, Malcha Marg,
Chanakyapuri,
Delhi-110021
Website: www.indiasmartgrid.org