About Me



NAME

Gahangir Hossain

TITLE

Professor

YEARS AT UNT

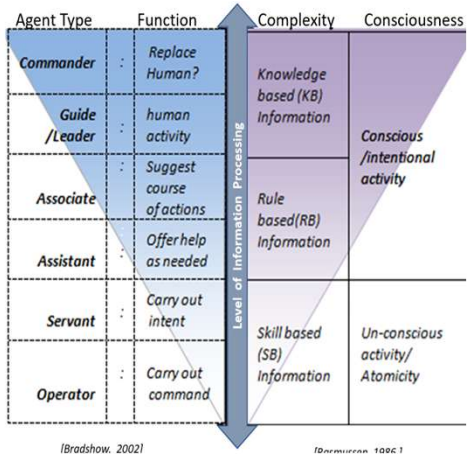
5

RESEARCH FOCUS AREAS

- Artificial Intelligence, Brain and Cognitive Science
- Data Visualization and Analytics
- Cybersecurity Management
- Cognitive System Engineering
- Machine Learning and Recommender Systems
- Health Informatics and Management

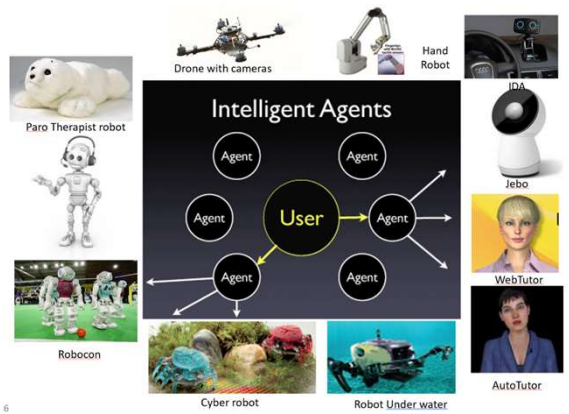
Cognitive AI Agents and Collaborative Sensemaking

1 AI AGENT ROLES & COGNITIVE CAPACITY



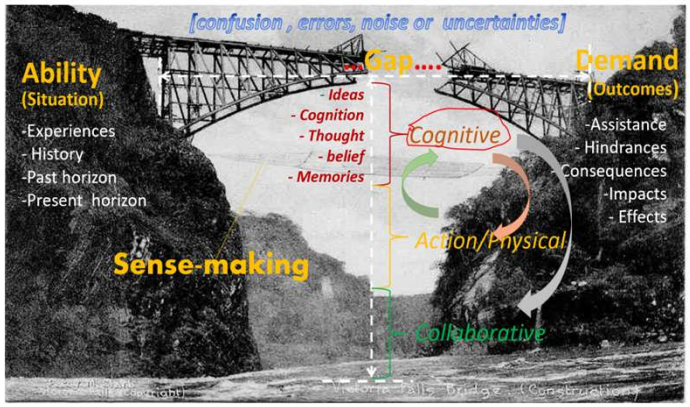
Operator → Assistant → Associate → Guide → Commander

2 HUMAN–AGENT COLLABORATION



Shared reasoning + dynamic role orchestration

3 CLOSING THE ABILITY–DEMAND GAP



Cognition • Action • Collaboration under uncertainty

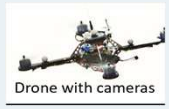
RESEARCH ARCHITECTURE

Sense & perceive → Interpret & share context → Negotiate & plan → Coordinate actions → Learn & adapt

Applications



Care



Autonomy



Robotics

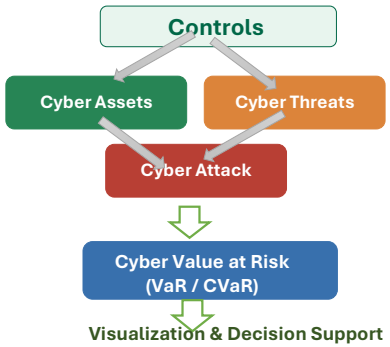
Continuous Cyber Risk Visibility & Verification

FOCUS AREAS | AI for Cybersecurity | Cybersecurity for AI

Use AI to quantify & verify cyber risk • Secure AI systems, agents, models, and data

1. Research Foundation

Translate cyber assets, threats, attacks, and controls into business-facing risk using Value at Risk (VaR) and Cyber Value at Risk (CVaR).



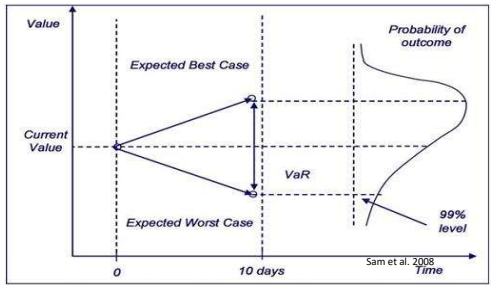


Selected directions

- Integration with Zero-Trust and SASE
- IoT anomaly risk assessment
- Cloud / multi-tenant cyber risk
- Insider-threat risk estimation
- Continuous control verification

2. Key VaR / CVaR Figures

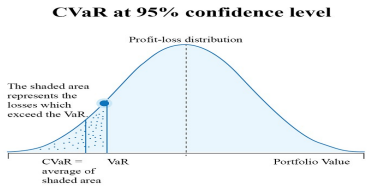
Value at Risk (VaR)



$$\text{Value at Risk} = v_m \frac{v_i}{v_{i-1}}$$

VaR estimates a loss threshold at a chosen confidence level.

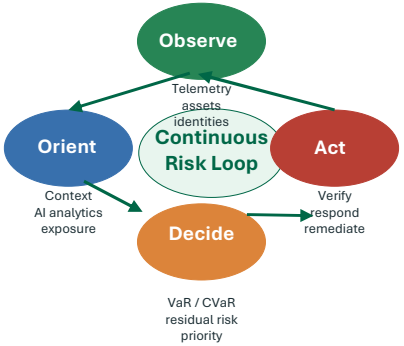
Cyber Value at Risk (CVaR)



CVaR focuses on expected loss beyond the VaR cutoff (tail risk).

3. Continuous Verification

A Cognitive Model, OODA-style loop can operationalize continuous cyber-risk visibility and verification.



Application Areas

Agriculture, Healthcare, Transportation, etc.

Applied in two directions

AI focused Cybersecurity

Detect risk faster

Agentic AI Security, Cognitive AI for Cyber Resilience, and AI-Driven Governance

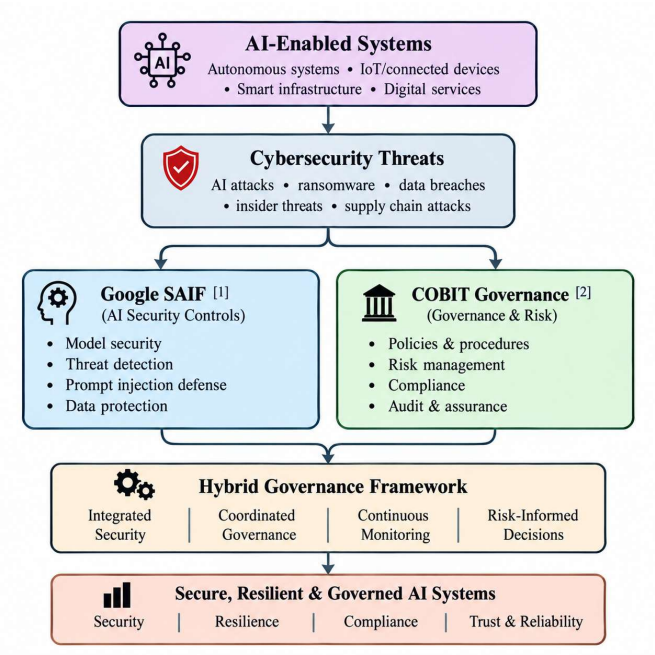
Cybersecurity focused AI

Protect AI assets

Cognitive, Trustworthy, Secure, and Resilient AI Systems

AI and Data Governance : Public Safety Recommendation

Digital twins + live sensing + predictive analytics for safer pedestrians, cyclists, and drivers



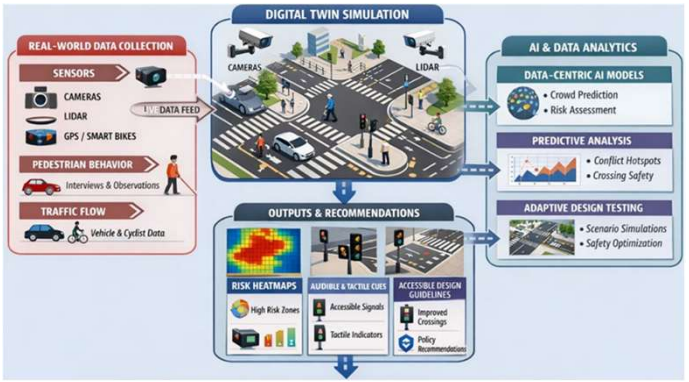
Hybrid Governance Framework

Public Safety: Research Focus

Create a protected-intersection intelligence layer that continuously learns from real-world traffic, simulates design alternatives, and recommends safety actions before conflicts become crashes.

Goal

Reduce conflict hotspots, improve crossing safety, and support accessible street design.



Concept workflow: sensing → digital twin → AI analytics → safety interventions

System Pipeline

01 Real-World Sensing

Cameras, LiDAR, GPS/smart bikes, pedestrian observations, traffic counts

→

02 Digital Twin Simulation

Dynamic protected-intersection model with live feeds and scenario testing

→

03 AI Risk Analytics

Conflict prediction, heatmaps, risk scoring, near-miss detection

→

04 Safety Recommendations

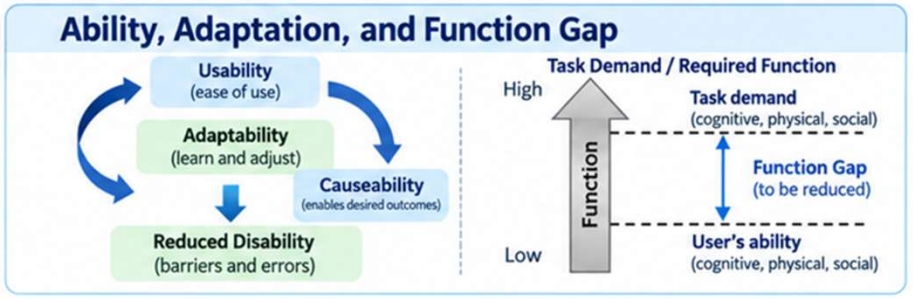
Signal timing, tactile/audio cues, design guidance, policy support

Expected Impact: evidence-based protected intersections that enhance public safety, accessibility, and trust in AI-enabled transportation.

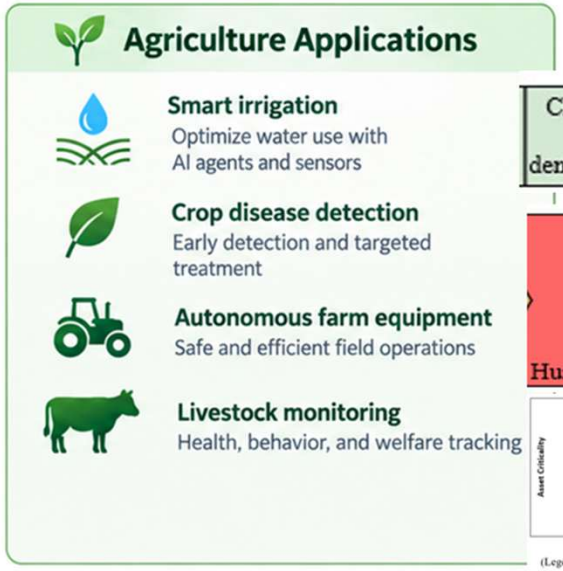
[1] Google, Secure AI Framework (SAIF), 2023. blog.google
[2] ISACA, COBIT 2019 Framework: Governance and Management Objectives, COBIT 2019. ISACA

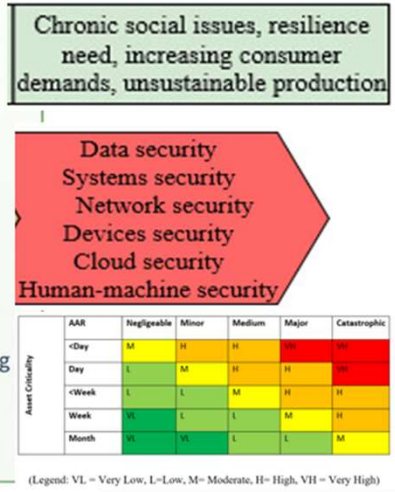
Cybersecurity for AI Agents in Agriculture 5.0







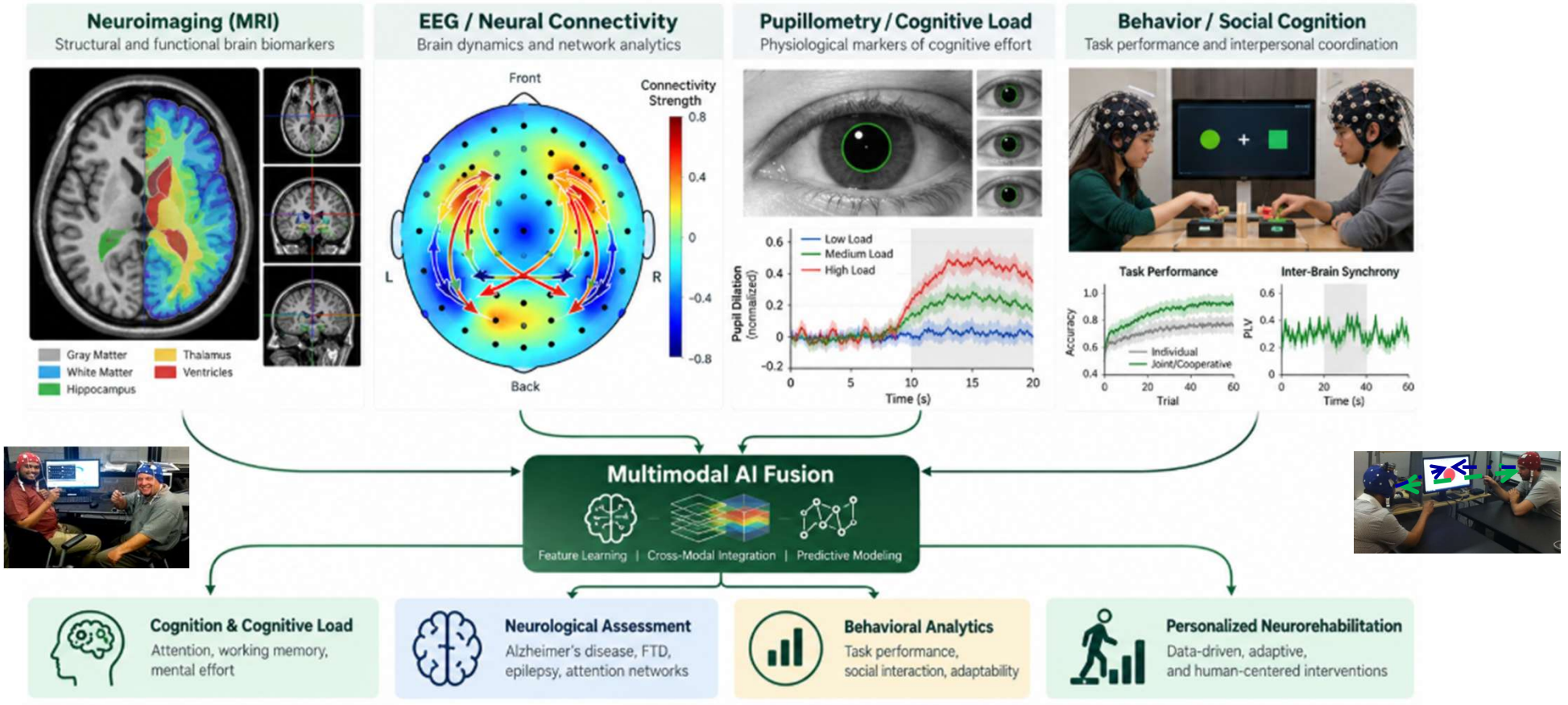






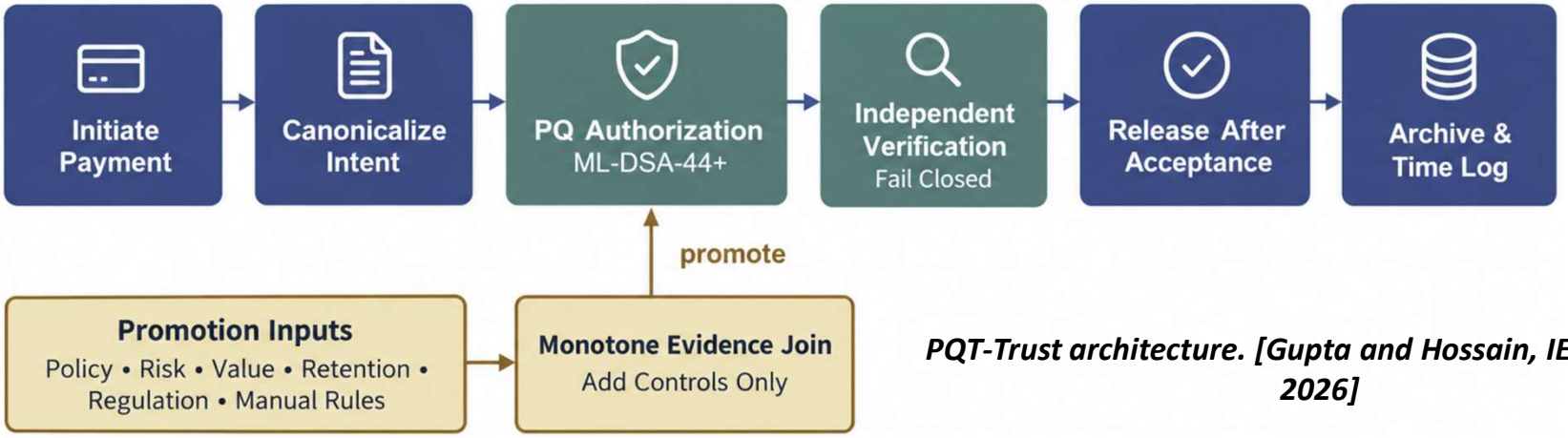
where $IARc_i$ is individual asset risk and $P(C_i)$ captures dependency influence.

Multimodal Brain & Behavioral Data Analytics

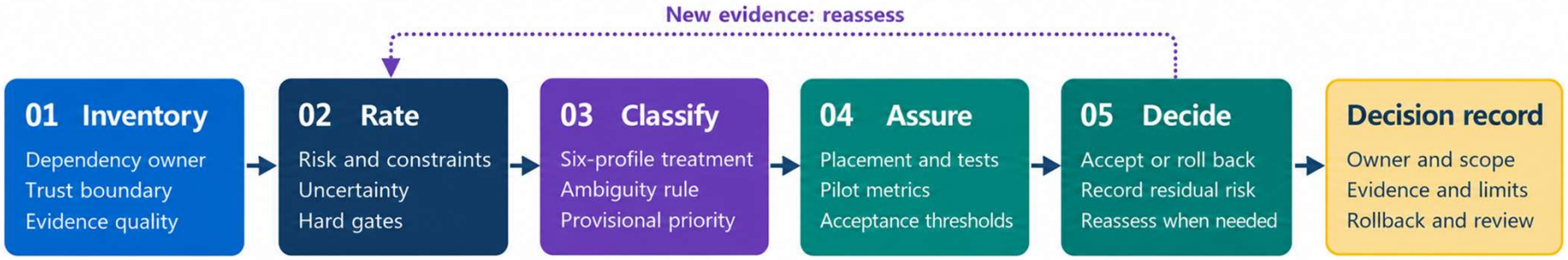


Applications: neurocognitive recovery • social-cognitive rehabilitation • attention / fatigue • problematic digital-media use

Post-Quantum Cryptography and Cyber Resilience



PQT-Trust architecture. [Gupta and Hossain, IEEE ACCESS 2026]



Telecom Quantum-Safe Migration Framework (T-QSMF) Workflow [Gupta and Hossain, Springe Discover Telecommunication 2026]