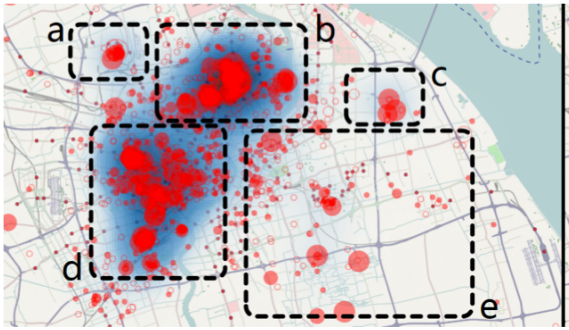


Social Media Activity

Physical Event Activity

Cyber Event Activity

Paul Rad, Ph.D.

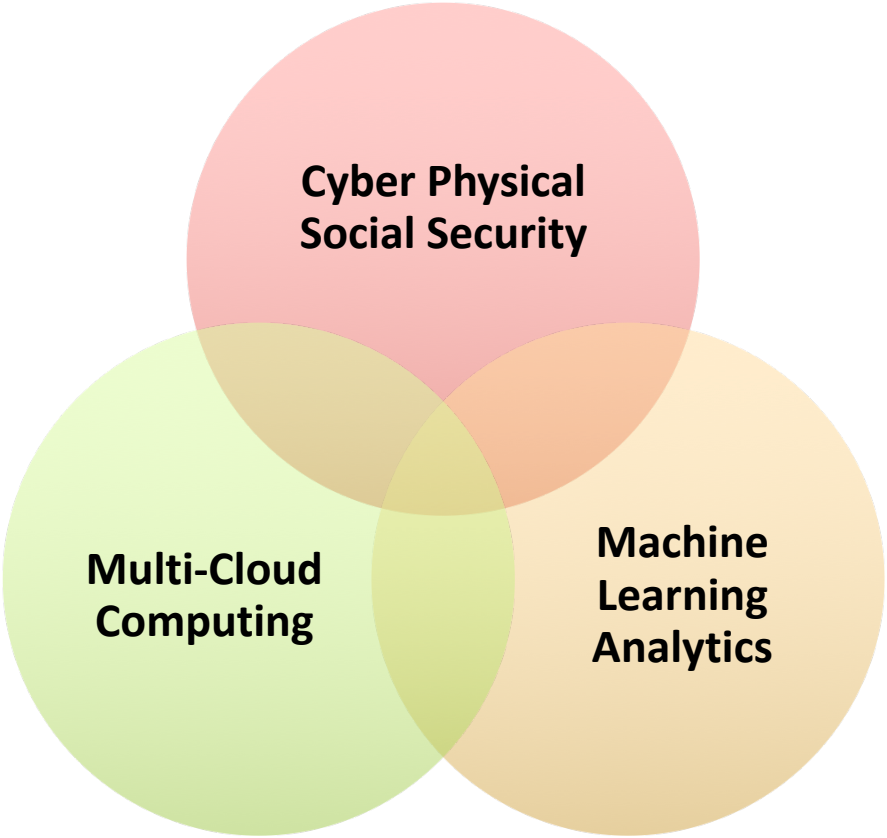
Associate Professor, Cyber Analytics
Department Information Systems and Cyber Security
Co-founder Open Cloud Institute (OCI)
Mobile: 210.872.7259

Agenda

- Open Cloud Institute (OCI)
- Cloud Machine Learning for BigData Analytics
- Video Analytics
- Cyber Autonomy and Decision Making
  - Autonomous Vehicles
  - Reinforcement & Behavior Learning
- High-Fidelity Visual and Physical Simulation
- Adversarial Machine Learning

Cyber Analytics Research

- Machine Learning Cloud and Data Analytics
  - Deep Learning and Reinforcement Learning
  - Adversarial machine learning
- Cyber Security Threat
  - Malware Encrypted
  - Multi Modal Biometrics (Biometric as a Service)
  - Behavior Modeling using Digital Twin and Sensors
  - Cyber-Physical Hunting - Analytics to Detect and Prevent Attacks in Real-time
- Autonomous Systems and Decision Making
  - Autonomous and Driverless Car
  - Decision Making and Adaptive Control



Cloud Computing Research

Funded Cloud Computing Research

2014-2019

$10* M	A configurable experimental environment for large-scale cloud research	NSF
$6.6* M	Building a high performance cloud for science and engineering research	NSF
$5* M	Testing, Evaluation, and Control of Heterogeneous Large Scale Systems of Autonomous Vehicles	U.S. Air Force
$100* K	A Cloud Computing Pipeline for Precision Medicine	SALSI
$ 230 K	Talent Pipeline OpenStack Developer	Intel
$ 25 K	Cloud Based Data Analytics and Machine Learning for Bioinformatics	UT Health Sciences
$ 500K	Cloud data analytics	Rackspace
$ 400* K	Forensics and Machine Learning Smart Grid	CPS
$105K	Cyber Physical Hunting	Cisco

* Collaborative research

Industry and Academic Research Collaboration

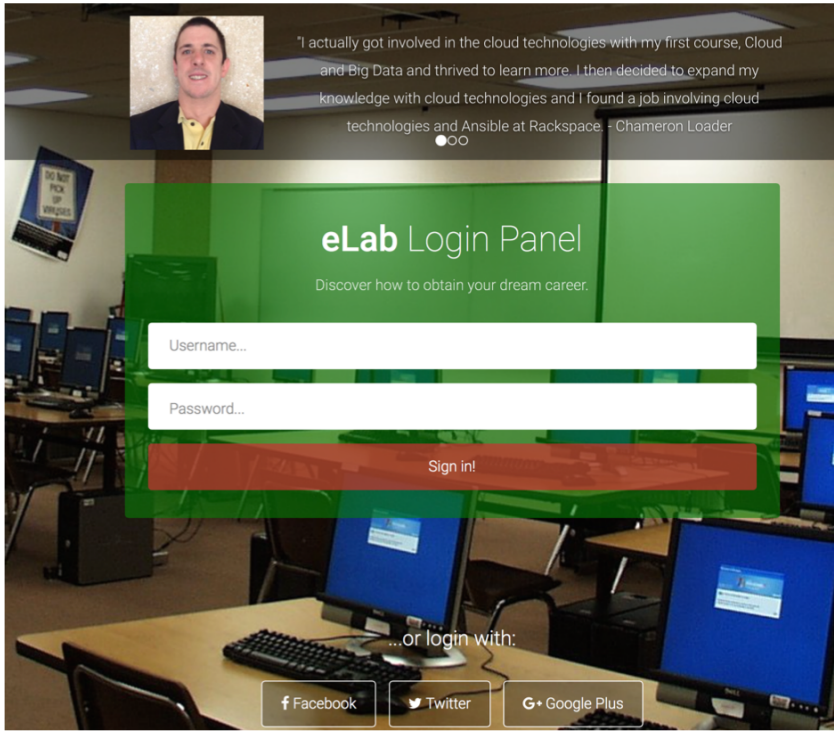
UTSA's partnerships and collaborations with industry, government and academia.

- OpenStack Foundation
- Open Compute Project (OCP)
- Rackspace
- Facebook
- Geekdom
- Intel
- NVIDIA "Research Center"
- Seagate
- Microsoft
- Amazon
- Mellanox
- Dell
- Cisco
- Georgia Institute of Tech.
- UT Austin
- University of Chicago
- UT Health Science Center
- University of Arizona
- Johns Hopkins University and Penn State University
- Cornell University
- Ohio State
- Cornell University

Cloud Computing Education

Cloud Computing Education

- **Cloud Computing Certification**
  - Cloud Security
  - Cloud Application
  - Cloud CORE Infrastructure
- **Industry Boot-camp Training and Certification**
  - "Intel OCI Internship" Cloud Computing Core OpenStack Infrastructure Programming.
- **Cloud Education Lab**
  www.cloudeLab.org
  - Working to build the best cyber and cloud technology education, innovation and workforce available anywhere.



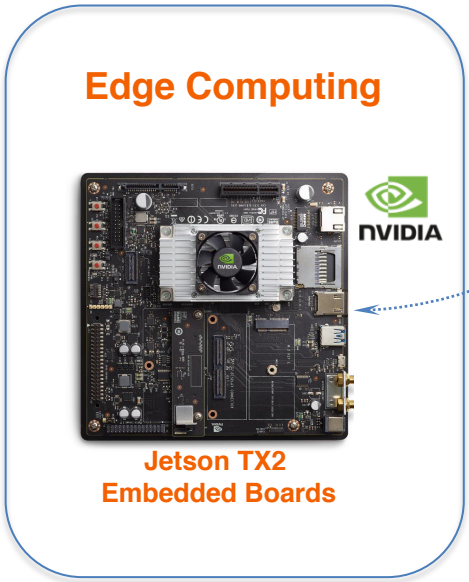
Research

Distributed Machine Learning over the Cloud, the Edge and Embedded Devices for Video Analytics

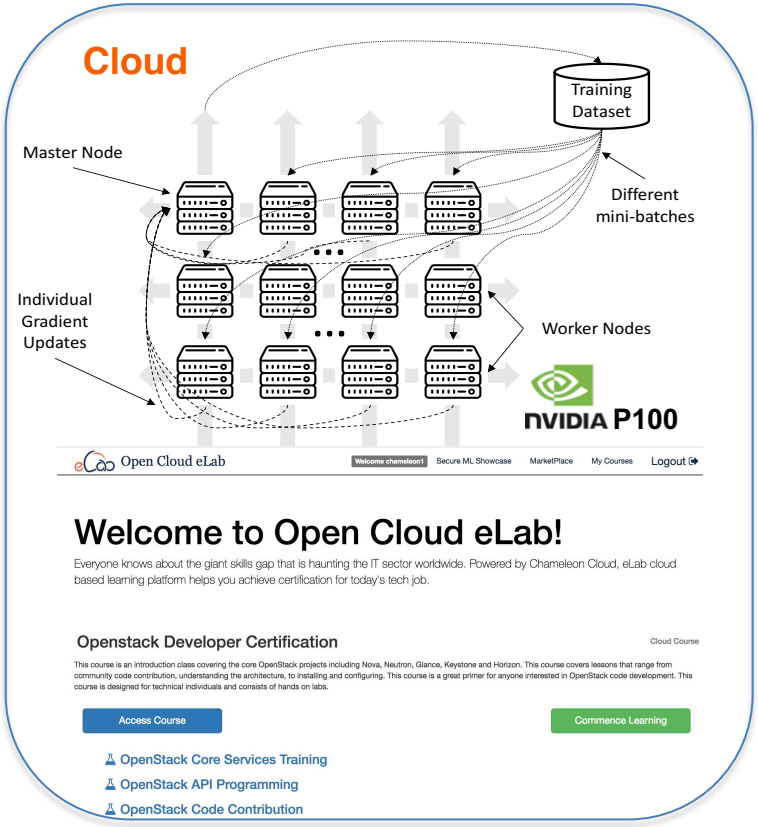
Research Objective

We propose distributed deep neural networks over distributed computing hierarchies, consisting of the cloud, the edge (fog) and end devices.

Methodology:



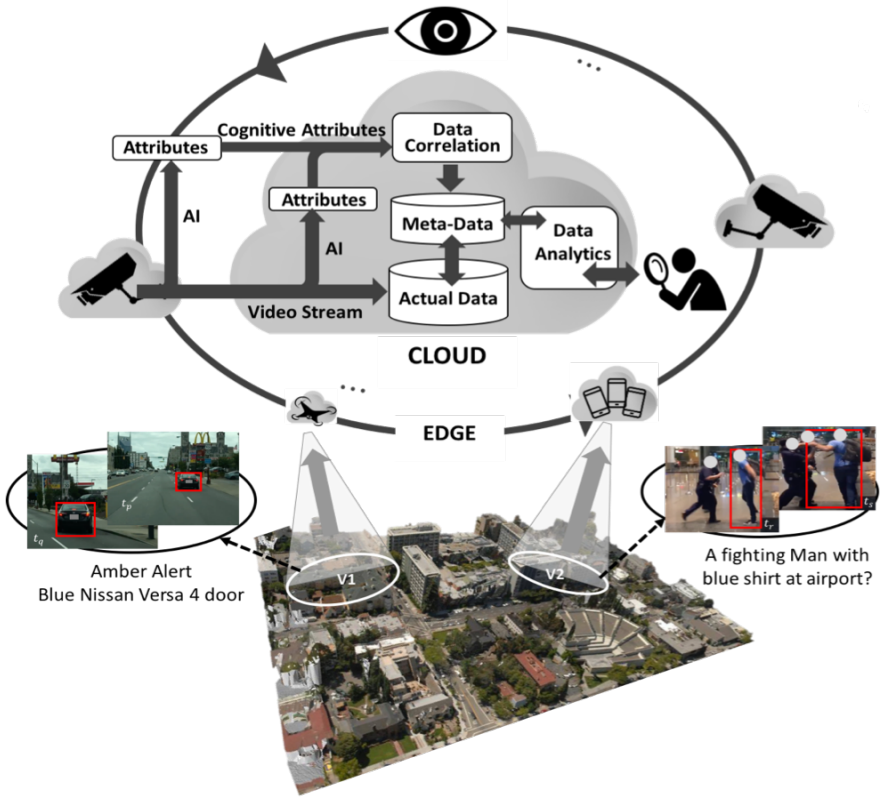
Trained ML Model



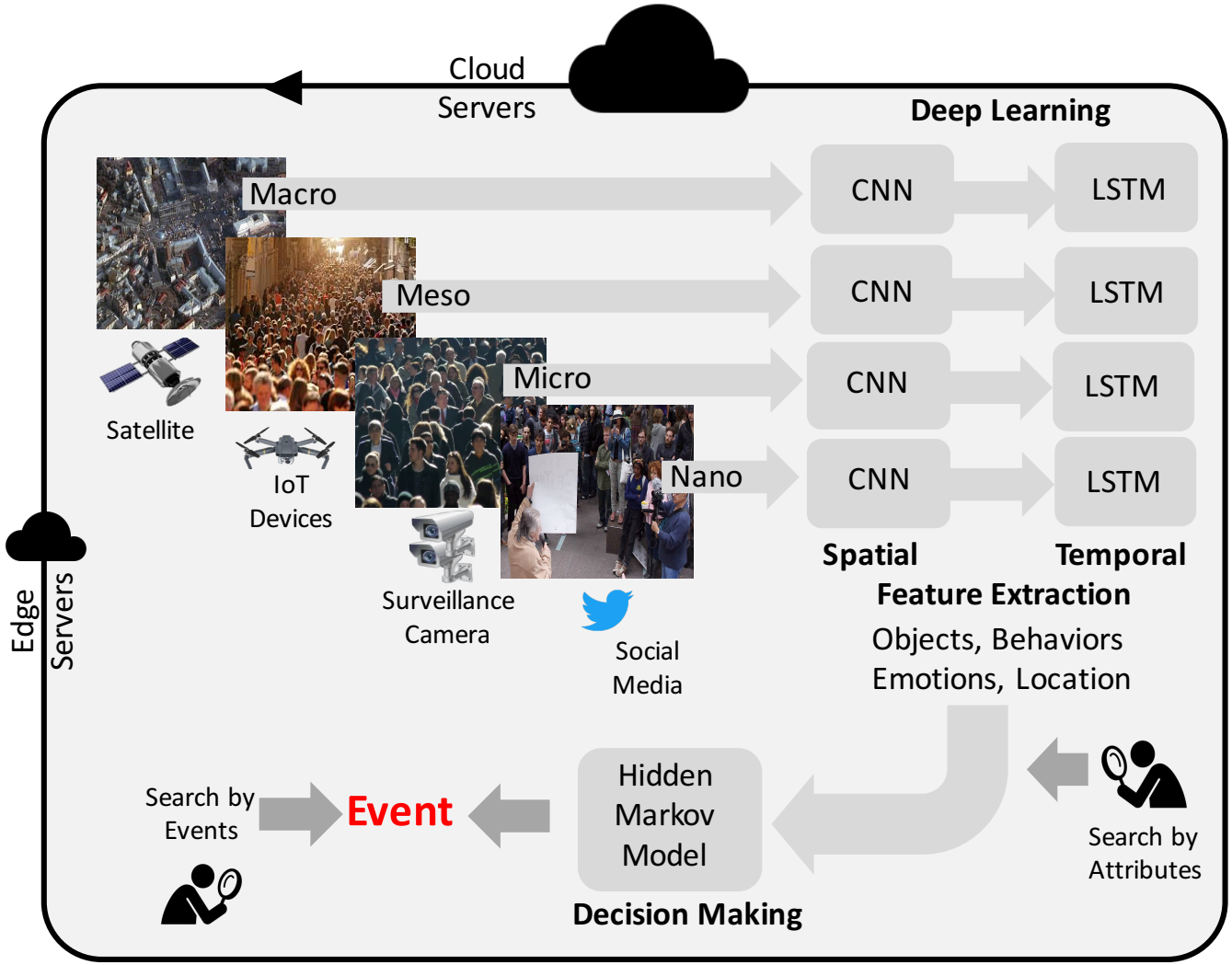
EYES: Cyber-Physical Hunting at Smart Cities Using Edge-to-Cloud Analytics

We propose EYES, a novel method of cyber-physical hunting to reduce the real-time semantic gap in automatic video interpretation and retrieval for not only simple images and features, but also rich and meaningful higher level interpretations of situations and events in images/videos stream captured from smart cities.

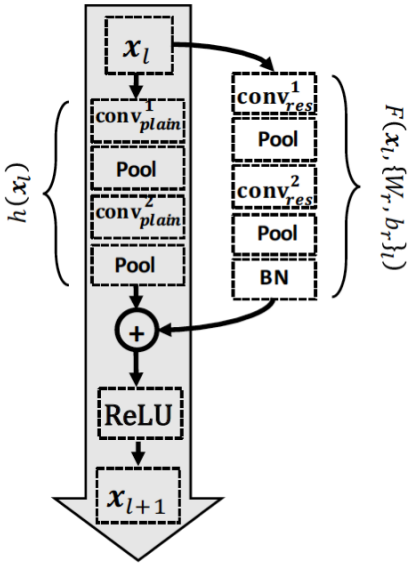
We will leverage previous developments in distributed cloud analytics that allow us to efficiently store and retrieve large quantities of video footage along with novel machine learning methods capable of interpreting those videos in a meaningful way



Cyber-Physical Threat Hunting at Scale

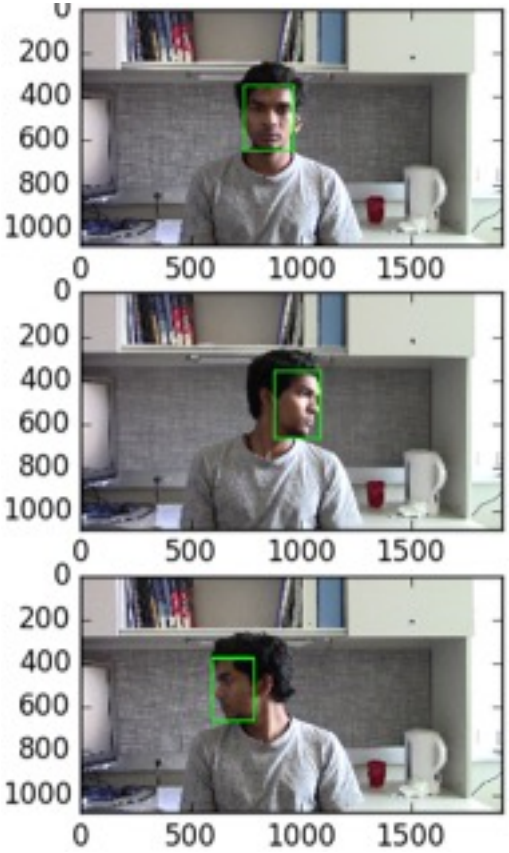


Crowd Facial Analytics



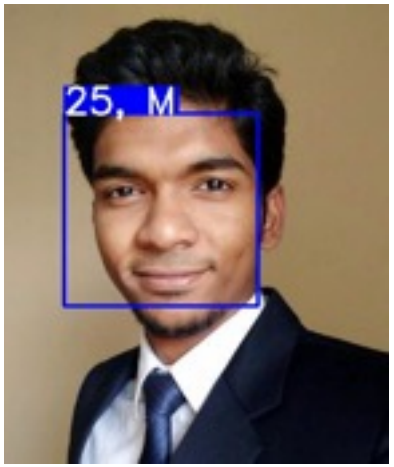
Face Re-identification, Emotion, Pose, Age, Gender

Face Recognition Different Pose

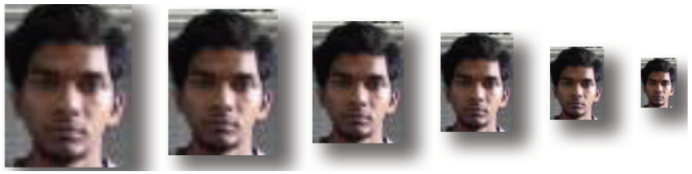


Face-Emotion Detection

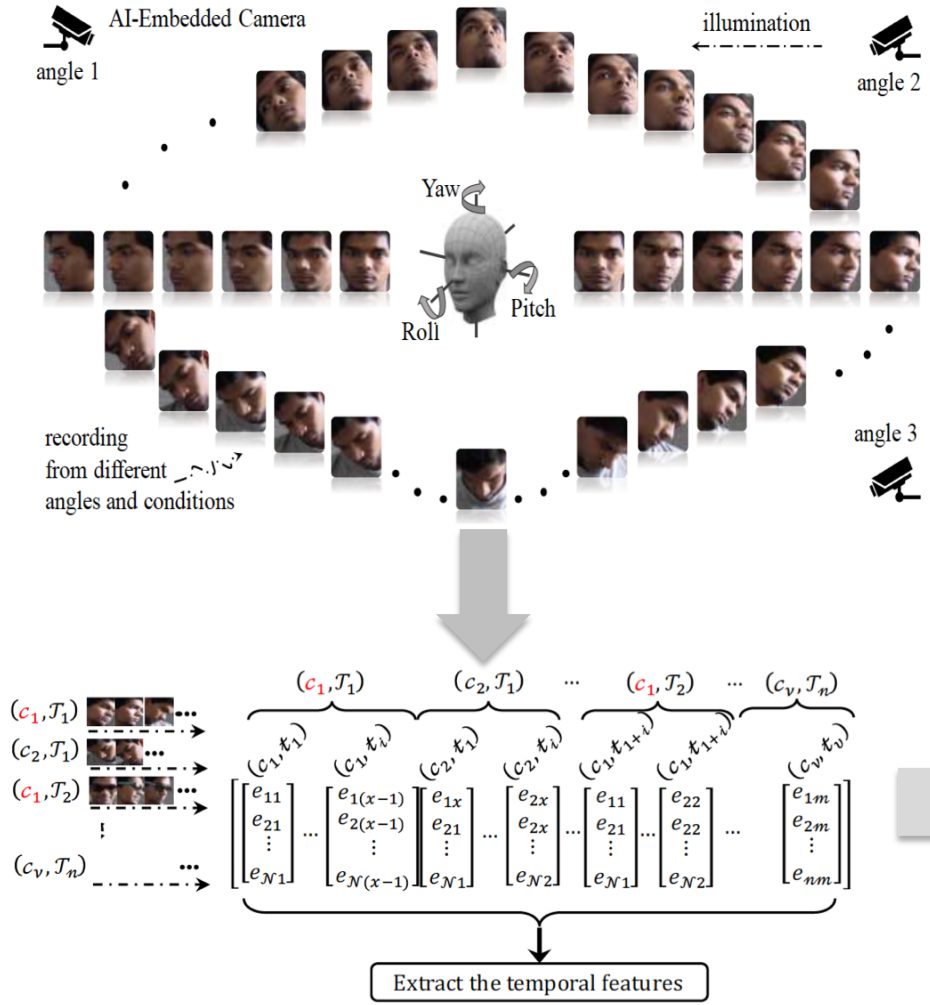
Face-Age-Gender

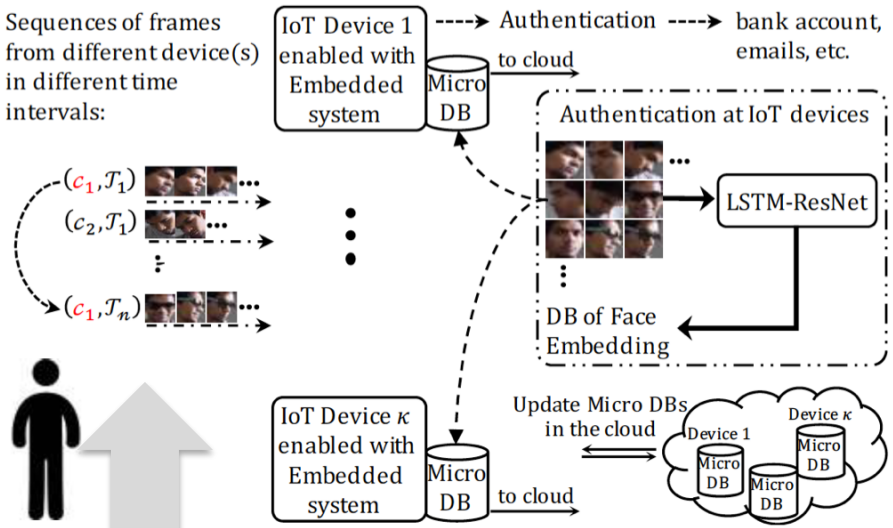


Face Recognition-Different scale



Decentralized ID: Blockchain + Embedding Biometrics





Connected Car: Driving Attention Monitor in Dangerous Road Conditions

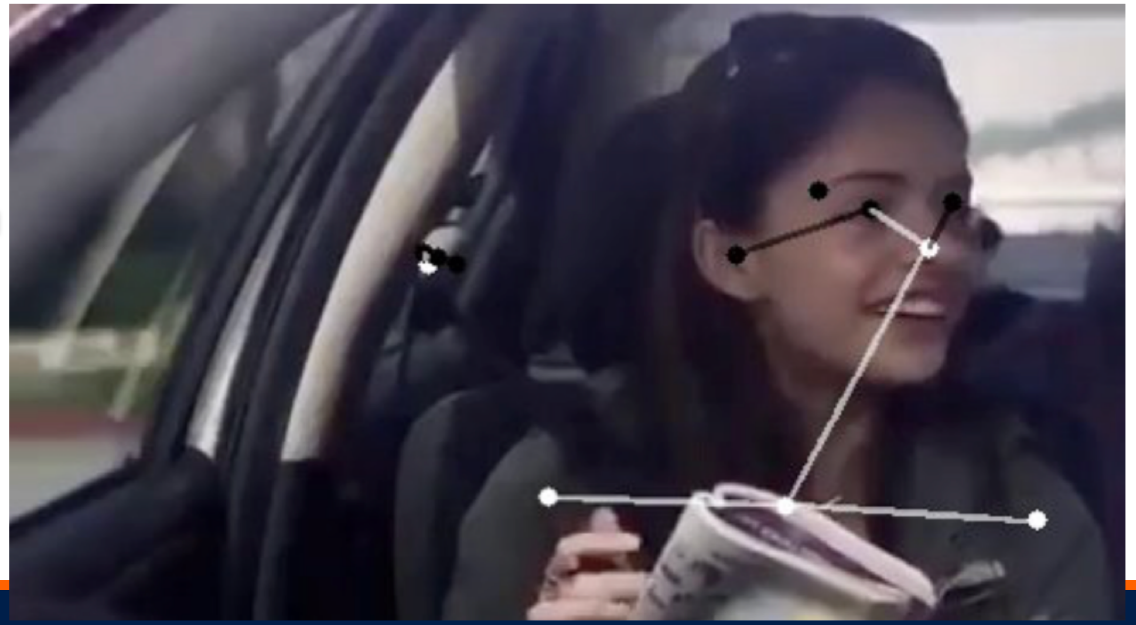
Research Objective

Simultaneous Situational assessment of driver attention and road condition in a connected car using Deep Learning.

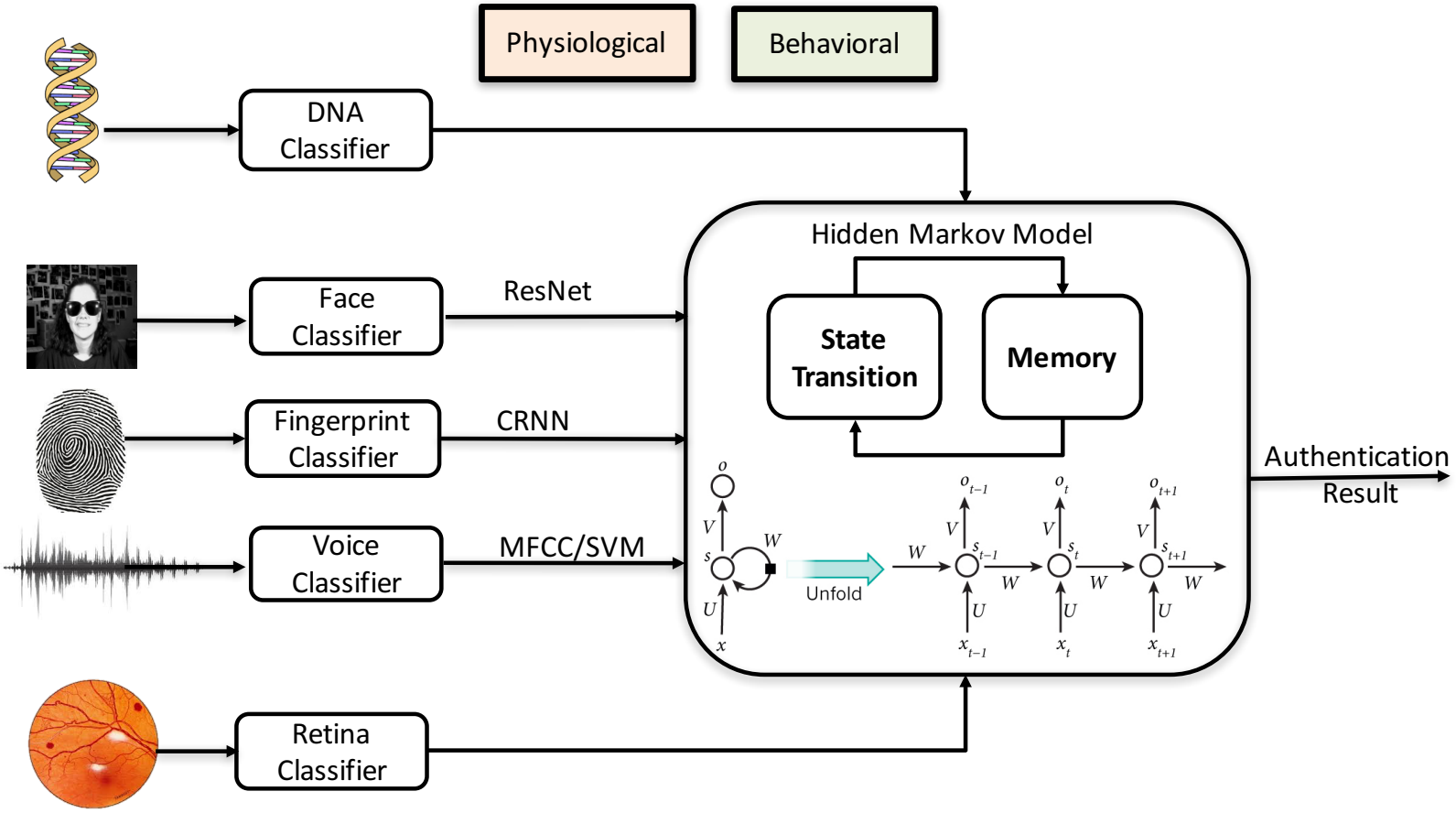
Methodology:

External Camera: Hazardous Object Detection

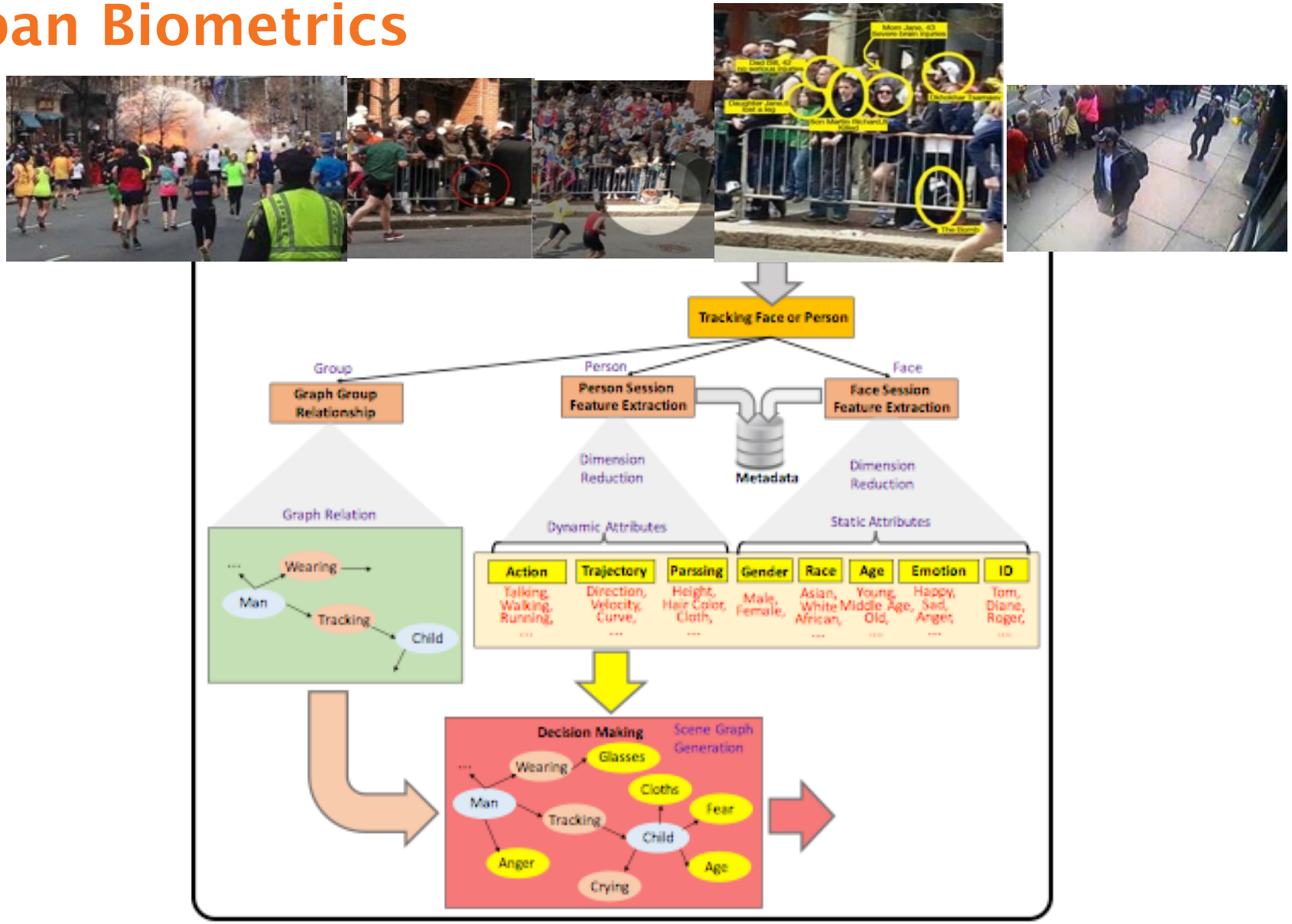
Internal Camera: Driver Attention Monitoring



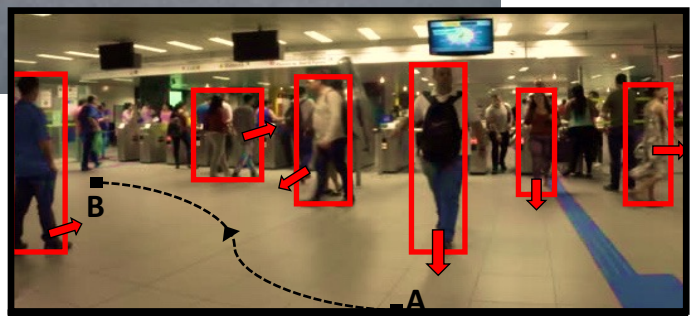
Biometrics as a Service

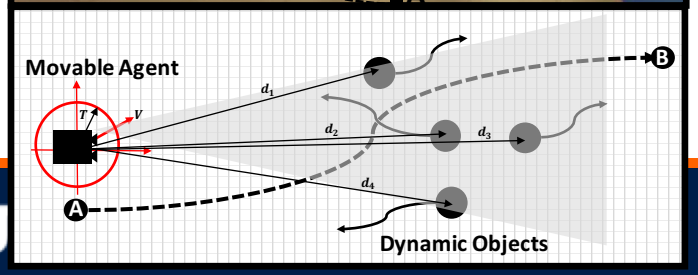


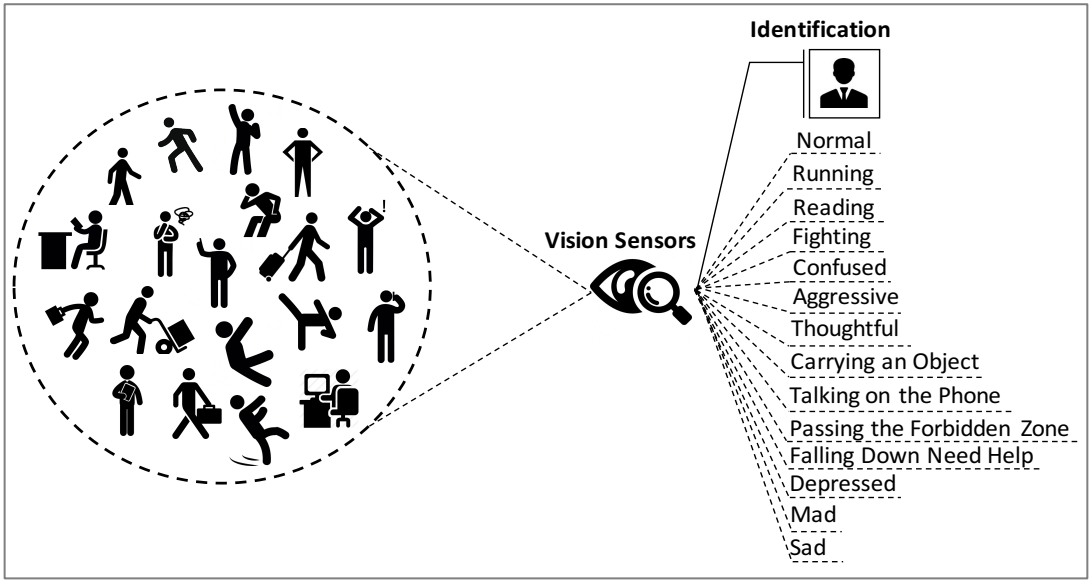
Urban Biometrics



Object Tracking Leading to Action Recognition







Personal Action detection

- Public responsibility
- Elderly home care
- Instant assistance and prevention

Suspicious behavior detection

- Loaf and run behavior
- Custom behavior detection model

Autonomous Decentralized Decision Making on UAV's for Team Mission

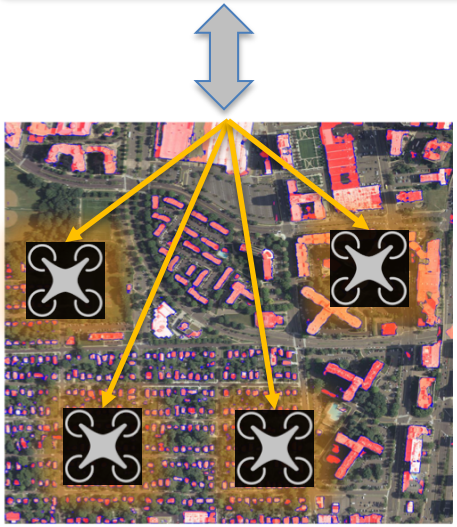
Research Objective

*Develop vision based **reinforcement control algorithms** capable of autonomous decision making and cooperatively achieve a global goal.*

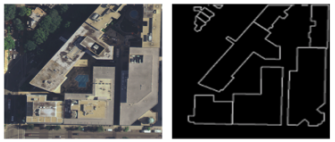
Methodology:

Disaster Areas - Satellite Images

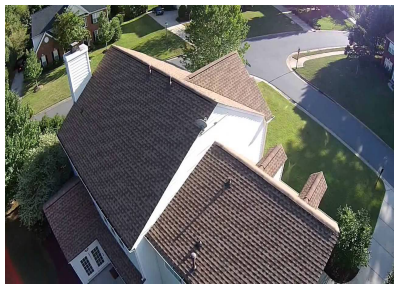
Human deployment + Supervisor Controller

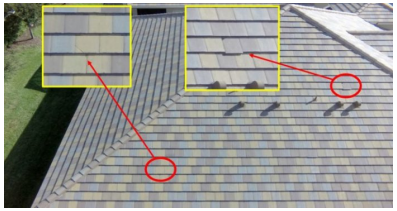


Drones deployed by human operator to disaster area, they form a team and independently cover desired location



The Drones combined images can be segmented into interest objects.

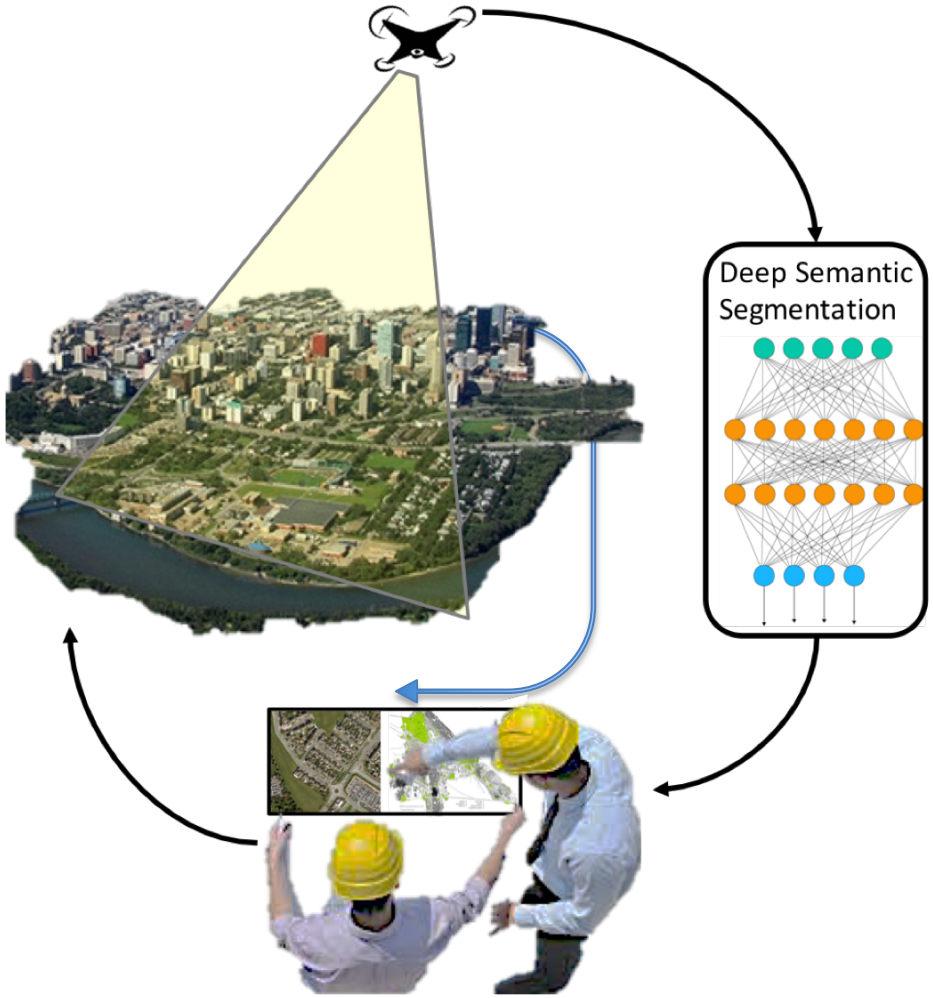


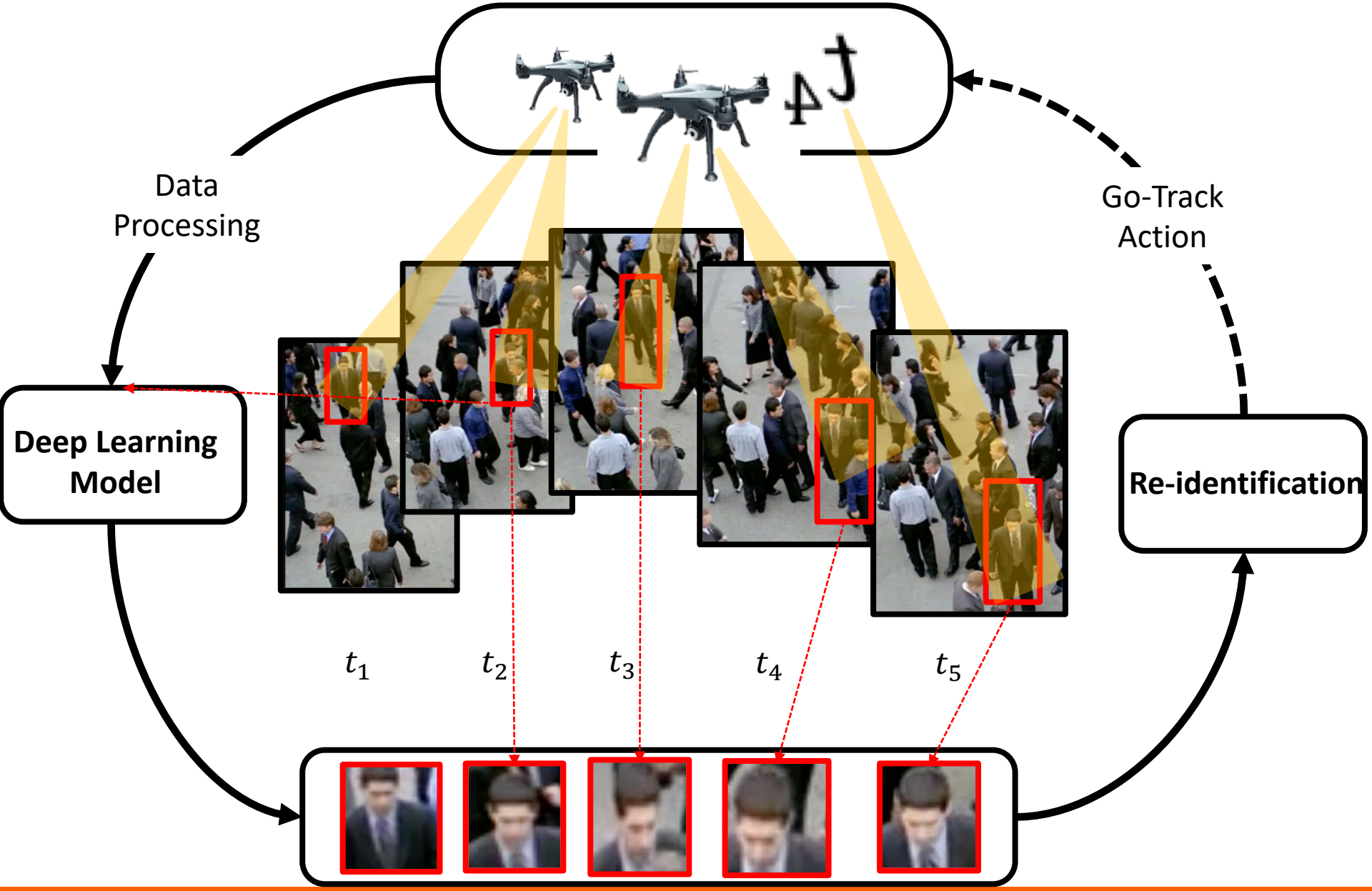


Each interest object can be further inspected for a detailed analysis.

Operator Interface – Address on Maps

Drone Reply with real-time pictures of the address




Data Processing
Go-Track Action
Deep Learning Model
Re-identification
t_1
t_2
t_3
t_4
t_5

Building Blocks of Autonomous Movement

Advanced decision systems interpret sensory information to identify appropriate navigation paths, as well as obstacles and relevant signage. Autonomous vehicles must have control systems that are capable of analyzing sensory data to distinguish between different objects on the road.

Sensor fusion
(Camera, LIDAR, GPS, etc.)

→

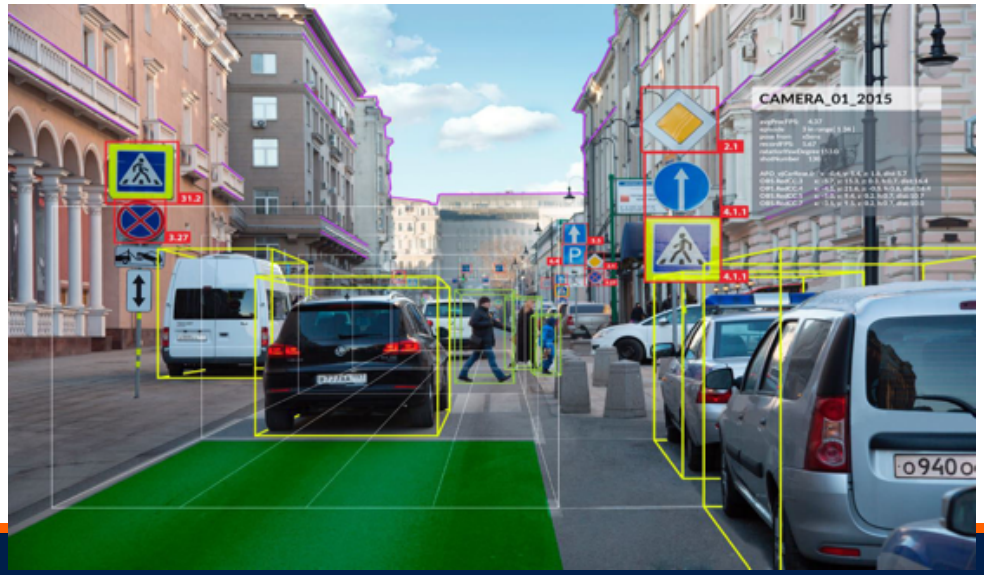
Perception
Object and Movement Detection and Classification

→

Vehicular Maneuvers
(Path Planning)

→

Actuator Control



Problem Solving Methods for Reinforcement Learning

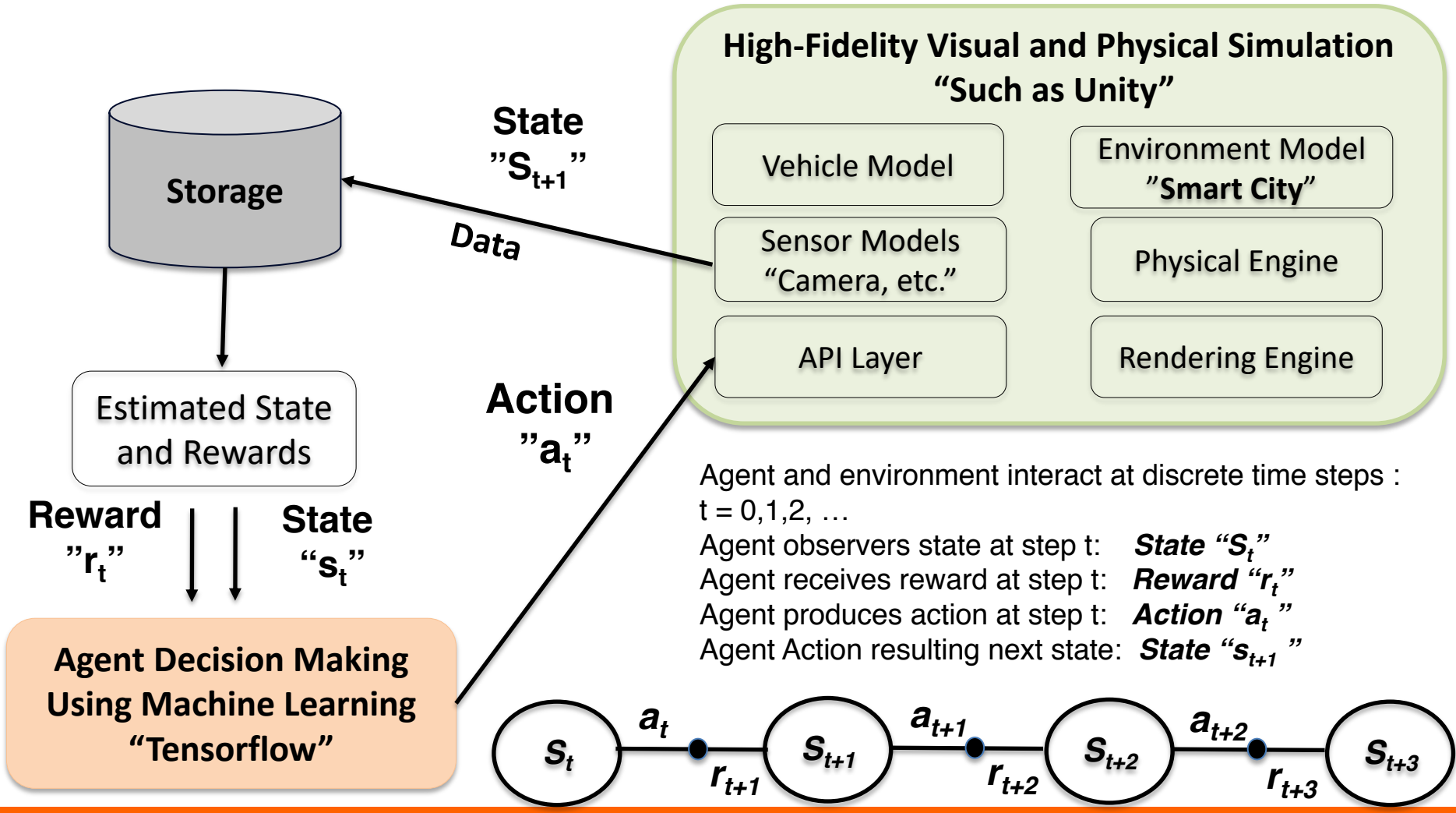
Paradigms such as reinforcement learning, learning-by-demonstration and transfer learning are proving a natural means to train various Autonomous Vehicles.

- Dynamic Programming
- Monte Carlo methods
- Temporal-difference learning

Building a Data-driven Autonomous Vehicles Key Challenges

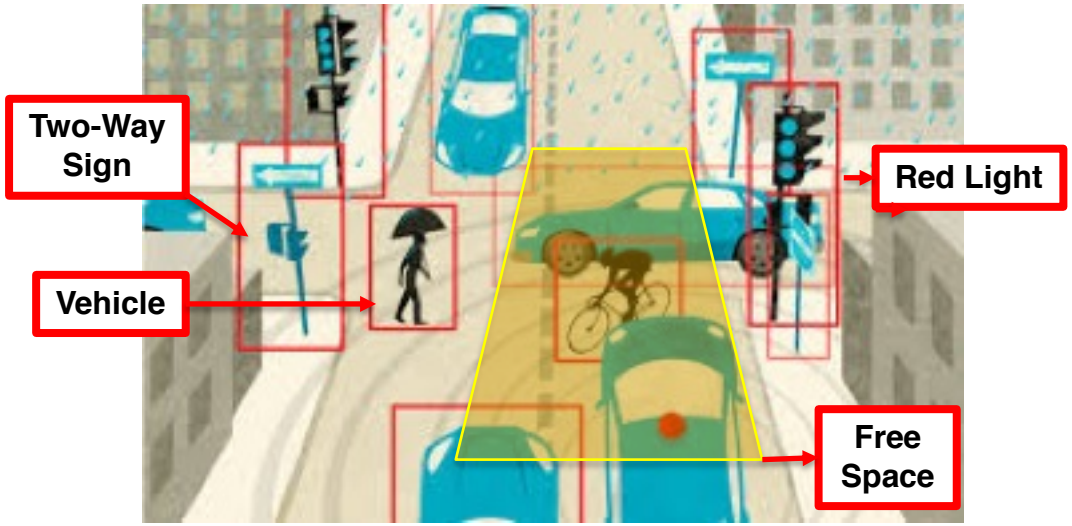
- Developing and testing algorithms for autonomous vehicles in real world is an expensive and time consuming process
- The high sample complexity – the amount of training data needed to learn useful behaviors is often prohibitively high
  - learn useful behaviors is often prohibitively high
  - often unsafe and expensive to operate during the training phase

High-Fidelity Visual and Physical Simulation to Address the Challenges

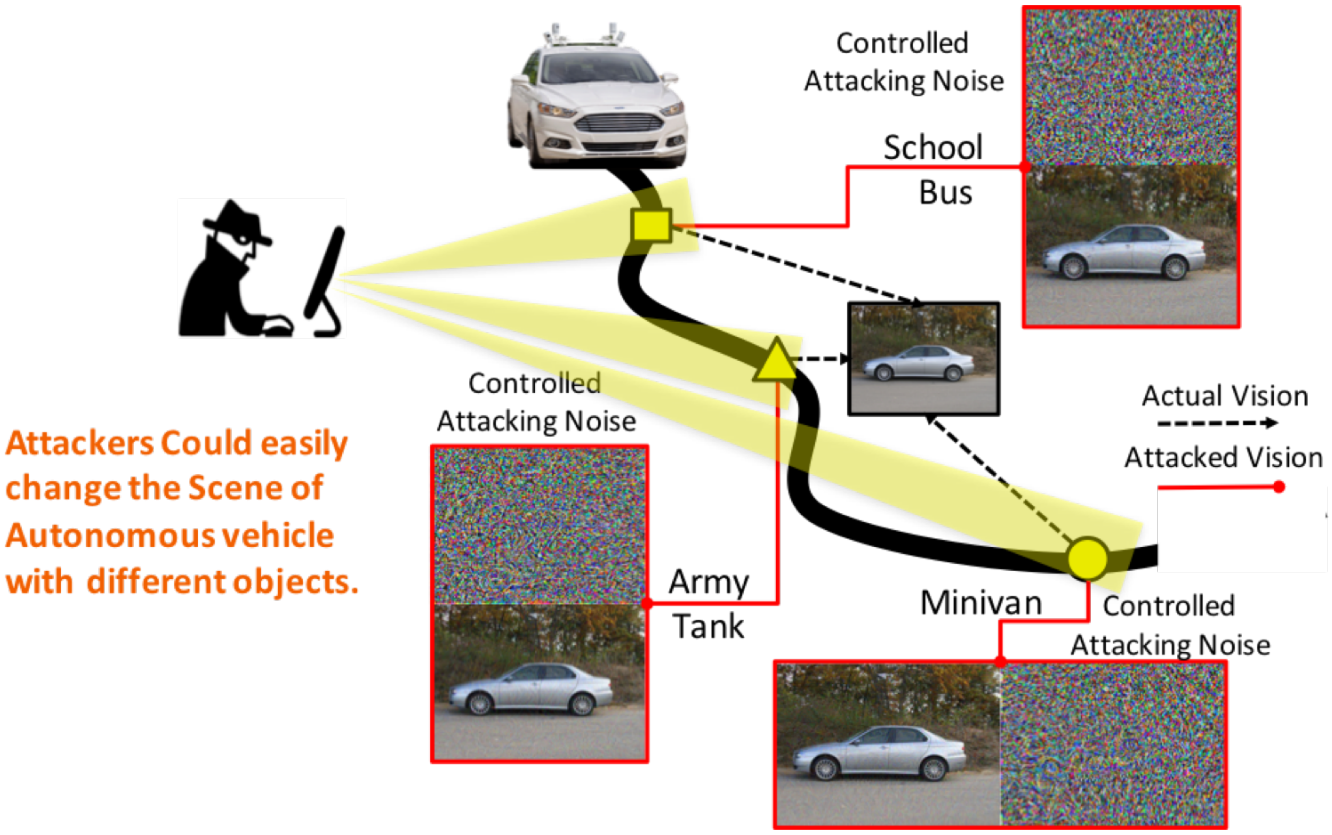


Adversarial Autonomous Vehicles

Autonomous vehicle use a variety of techniques to detect their surroundings, such as radar, laser light, GPS, odometry and computer vision. Advanced decision systems interpret sensory information to identify appropriate navigation paths, as well as obstacles and relevant signage.



Adversarial Autonomous Vehicles



Attackers Could easily change the Scene of Autonomous vehicle with different objects.

Adversarial Examples: Reinforcement Learning in Autonomous Vehicles

Reinforcement learning techniques based on Deep Q-Networks (DQNs) are also vulnerable to adversarial input perturbations. The attacker has no direct influence on the target's architecture and parameters, including its reward function and the optimization mechanism.
The only parameter that the attacker can directly manipulate is the configuration of the environment observed by the target.