CyberSafety and Systems Support for AI at the Edge

Shiv Mishra

Professor

Computer Science, CU-Boulder

Office: Systems lab: ECCR 1B22

Email: mishras@colorado.edu

http://www.cs.colorado.edu/~mishras

Current Research Focus

- System support for IoT
- Social Computing

System Support for Edge Computing

Inter-container Communication

Distributed Scheduling at the Edge

Smart Agriculture

CyberSafety

Hate speech in Arabic social media

Snapchat as a Lens on Public Health

Radicalization by YouTube's Recommendation Algorithm

Democracy and Technology

Impact of Russian bots

Misleading news and critical thinking

Resilience and Interventions

Socio-Technical Systems

Impact of Planned Disruptions

Health and social wellbeing

Environmental justice communities

System Support for Edge Computing

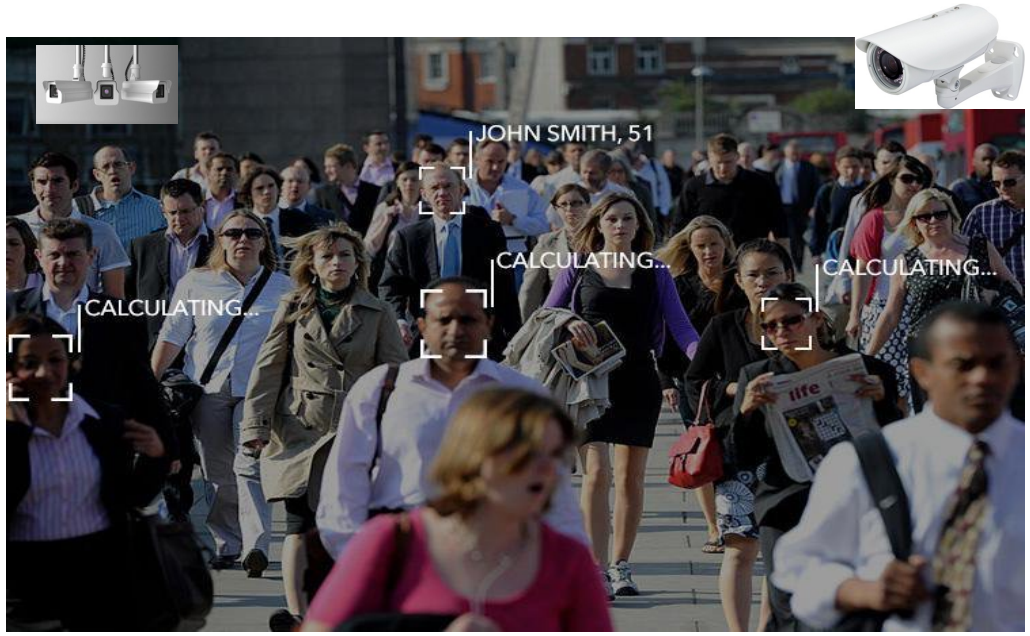
Problem: Augmented Reality

Task: To overlay useful labels over objects in a video stream

Data: Large volume, privacy-sensitive, location-sensitive, limited lifetime

Computation: Live video stream capture and frame segmentation, object recognition, information overlay, …
Requirements: Compute intensive, context aware, real time, privacy preserving

Problem: Identifying and tracking people



Task: To identify and track people in a moving crowd in real time

Data: Large volume, multiple sources, location-specific, privacy-sensitive, limited lifetime

Computation: Face recognition and tracking

Requirements: Compute intensive, context aware, real time, privacy preserving

Problem: Smart Agriculture

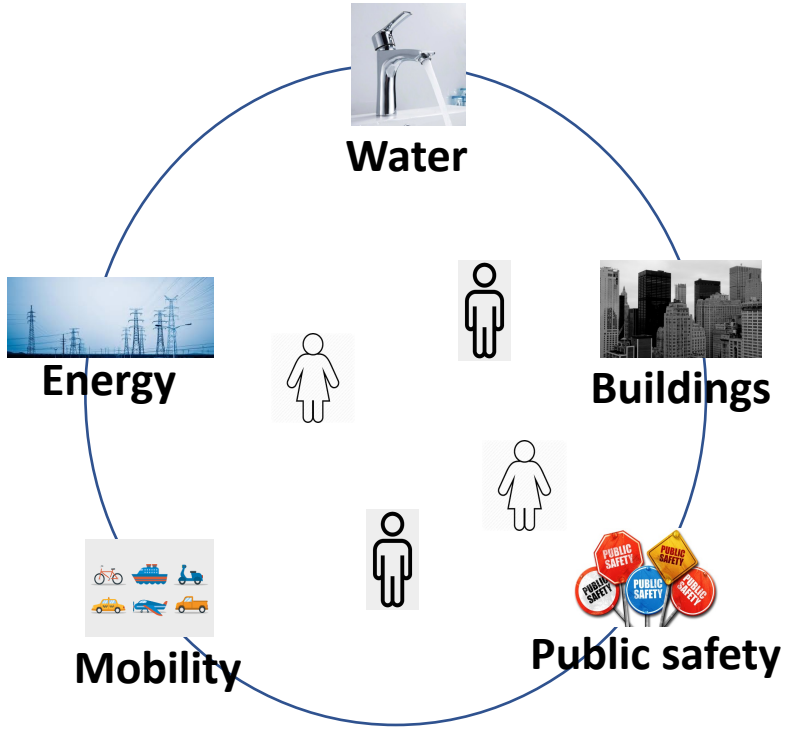
Task: Smart irrigation, fertilizer application, crop disease prevention, locating weeds, …

Data: Large volume, multiple sources, hybrid, location-specific, limited lifetime

Computation: Pattern recognition, anomaly detection

Requirements: Compute intensive, context aware, near real time

Problem: Management of city operations



Task: Optimal water and energy distribution, traffic management, smart buildings, public safety, …

Data: Large volume, multiple sources, hybrid, location-specific, limited lifetime, privacy sensitive

Computation: Optimization, anomaly detection, context aware
Requirements: Compute intensive, context aware, real or near real time, privacy preserving

IoT Environment

Personal air Pollution sensor

Environment sensor

Camera

Autonomous car

Smart watch

Robot

Health monitor

Smartphone

Static and mobile sensors are generating lots of sensor data in real time

Goal: To provide highly sophisticated, personalized, context-aware services in (near) real time *with humans in the loop*

IoT Environment

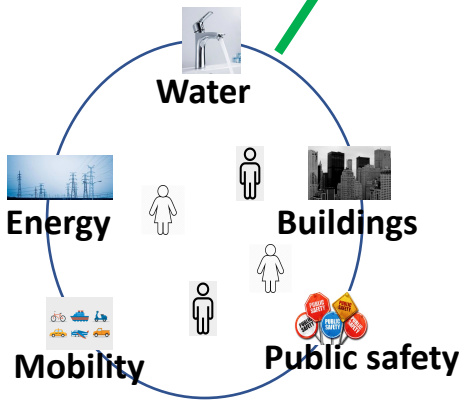
Key Question: Where to collect and process the sensor data to build sophisticated, context-aware services?

- Onsite Computing
  - Limited resources (power, CPU, memory), device heterogeneity
- Computing in the Cloud
  - High latency, high bandwidth consumption, privacy leakage, lost context, …
- Edge Computing
  - Put services and resources of the cloud closer to users, possibly with in one wireless hop

Edge Computing

Edge Server: CPU, GPU, FPGA, …

- Data center in a box, closer to the sensors
- Represents the middle tier of a 3-tier hierarchy: onsite – edge - cloud



Edge computing: Low latency, low bandwidth consumption, separate administrative domains, security & privacy

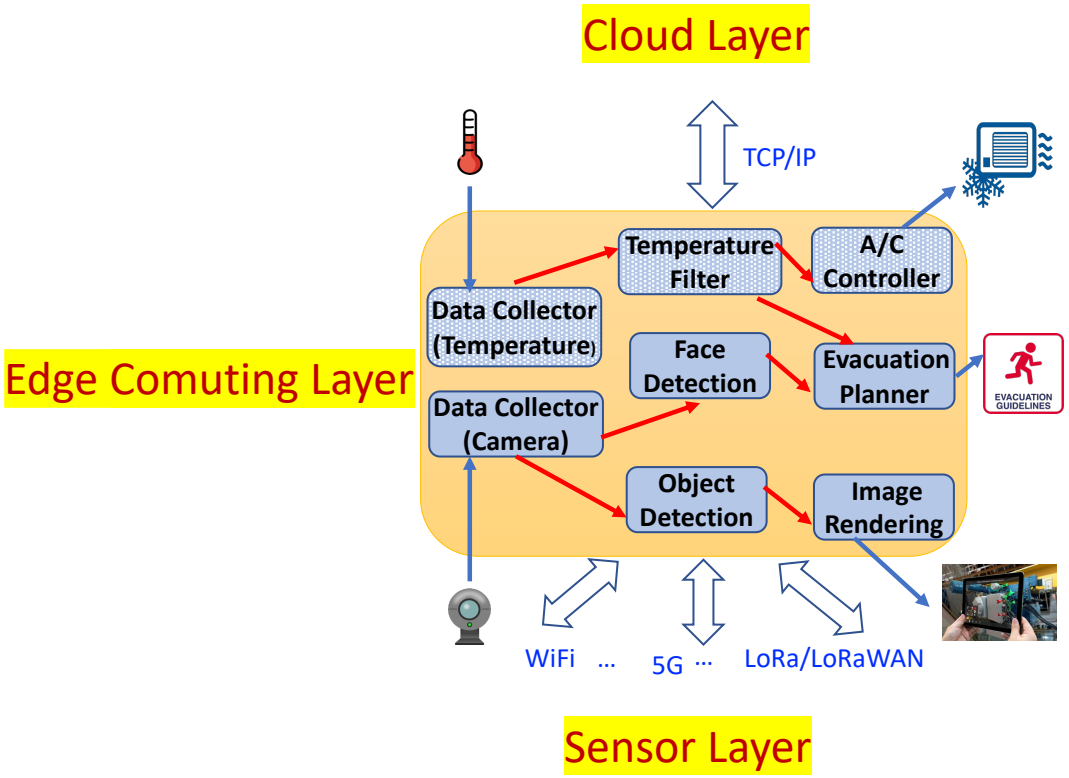
Edge Computing

Key driving technology for building sophisticated, context-aware, real (or near real) time IoT and smart city services

Edge Computing: Challenges

- Building sophisticated, context-aware applications at the edge is a complex task at present
  - Lack of any integrated system level support available to configure these applications
  - Heterogeneity of computing resources and sensing devices at the edge
  - Dynamic nature of the computing environment with mobile as well as static computing devices
  - Lack of trust among the collaborating entities
  - Minimal support to manage resource sharing

Research Goal: To develop and evaluate system level services to enable an efficient *microservice-based architecture at the edge*



- An application is implemented by composing a set of "microservices"
- Each microservice implements a basic functionality
- A microservice runs in an "isolated" computing environment
  - LXC, dockers, etc.
- Scale each microservice up or down

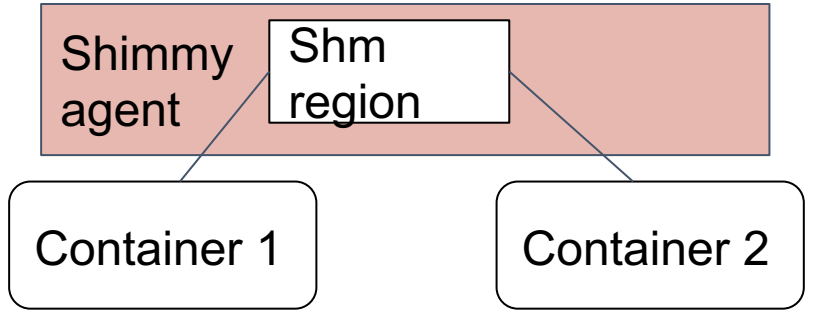
Edge Computing: Inter-Container Communication

- Observation: Inter-container communication is a key bottleneck in the application's performance
- Solution: Use shared memory channels
  - Bi-directional streams (as in TCP/IP) or publish/subscribe channels
  - Co-located containers:

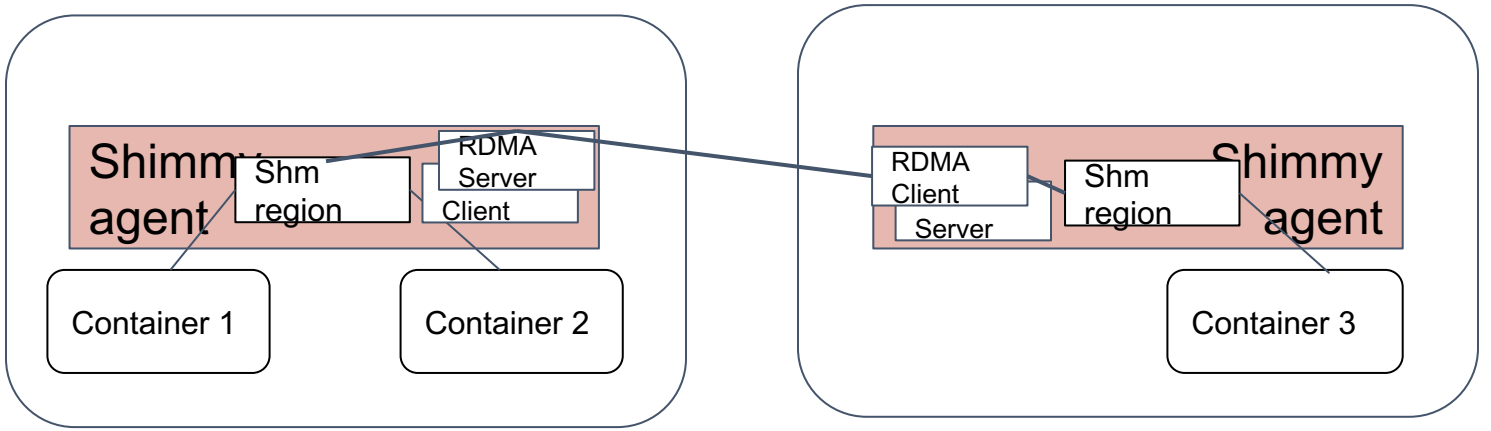
    hostIPC = true

  - Remote communication by synchronizing memory regions via Remote Direct Memory Access (RDMA) *(in progress)*
- Integrated with Kubernetes

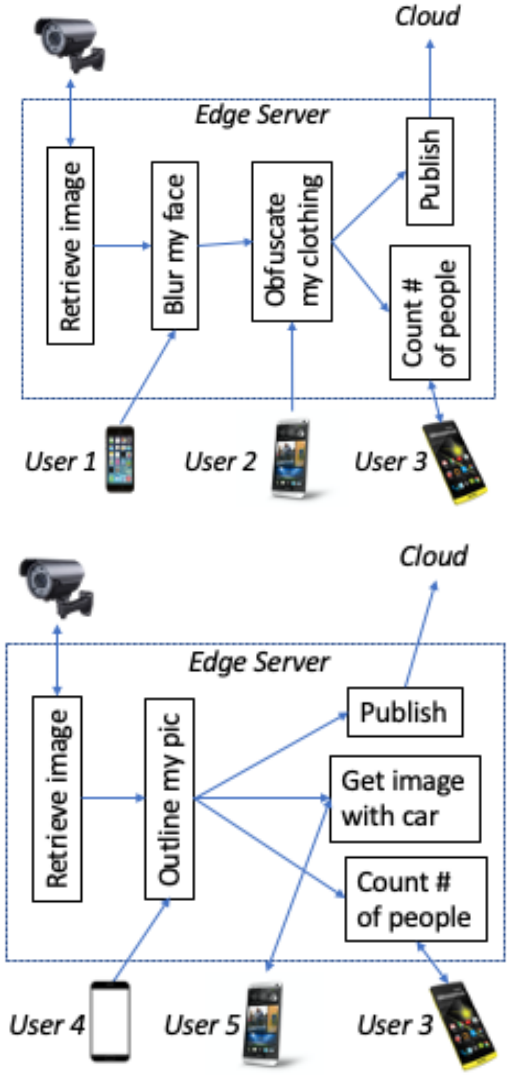
Local communication



Remote communication



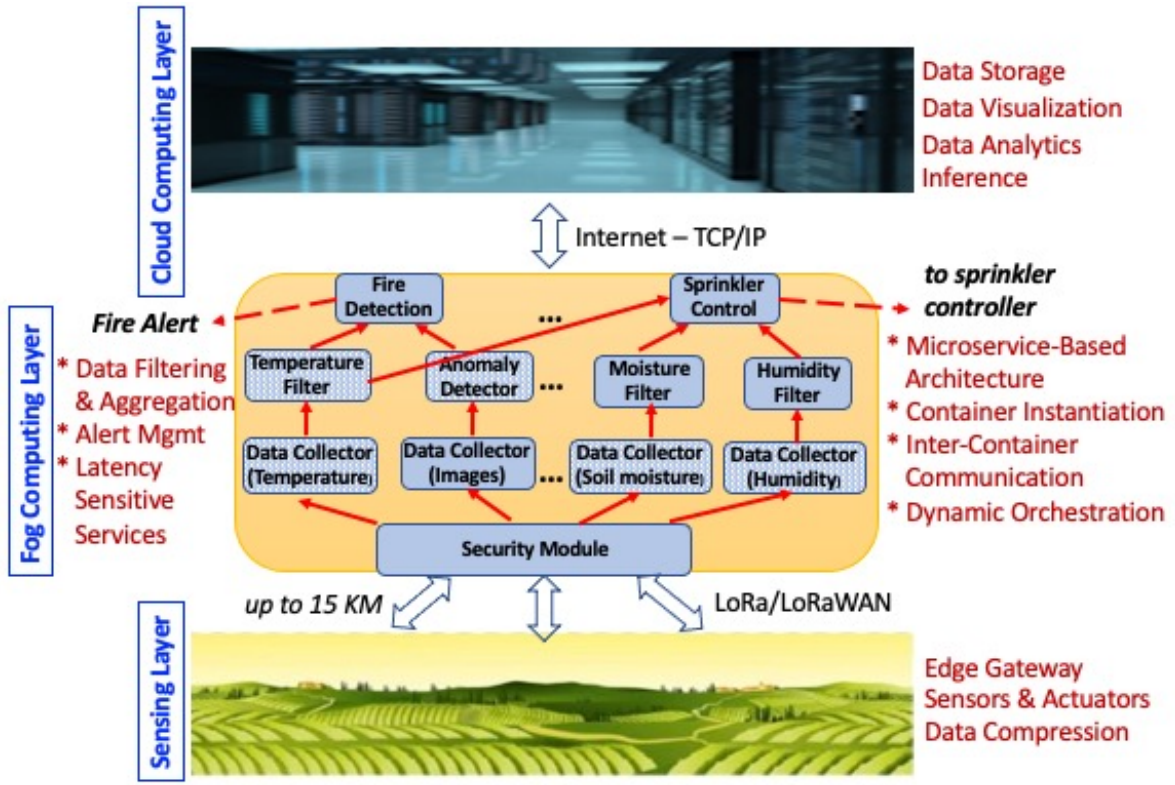
Edge Computing: Container Graphs



- Problem: any architectural level change in Kubernetes incurs service disruption
- Solution: Dynamic container instantiation & orchestration
  - Dynamic instantiation or removal of micro-services
  - Dynamic alteration of communication pattern among micro-services
  - Current application operation or its data-flow remains undisturbed
  - No application downtime
  - Kubernetes compatible

Edge Computing: Smart Agriculture

- To develop an end-to-end, LoRa-enabled, edge-based infrastructure for smart agriculture in India and USA
- Sensing layer: sense the agriculture field parameters and communicate them to Fog layer using LoRa
- Fog layer: provide support for latency-sensitive services as well as operation in a disconnected environment
- Cloud layer: Complex, compute-intensive decision making and long-term data storage and visualization.



Edge Computing: Distributed Scheduling

- A scheduler that schedules tasks among multiple heterogeneous processors to satisfy application's constraints
- Application constraints: deadlines, privacy, cost, …
- Processors: Low-end devices, CPUs, GPUs, FPGAs, …
- Challenge: How to keep the overhead of "making scheduling decisions" low

Edge Computing: Privacy

- Several privacy-at-the-edge related projects
  - Individual and group-based privacy negotiation mechanisms at the edge
  - Privacy leakage in home automation systems
  - Support for monitoring GDPR (General Data Protection Regulation) policies in IoT systems

- Contributors
  - Current Students: Fei Hu, Md. Rezwanur Rahman, Jinpeng Miao, Chris Godley, Kunal Mehta, Nisha Murarka
  - Khaled Alanezi , Mohammed Al-Mutawa
  - Sepideh Goodarzy, Maziyar Nazari, Marcelo Abranches
  - Vasu Sharma, Mana Khasgiwale, Prashanth Thipparthy, Hamza Motiwalla, Meeti Baliga, Biljith Thadichi, Srihaasa Pidikiti, Hima Boddupalli

Social Computing

CyberSafety: Introduction

- Problematic issues that arise while surfing the Internet
- Examples: Cyberbullying, obscene content, misinformation, propaganda, …
- Goal: To develop tools to automatically detect cybersafety issues, assess their impact, and techniques to mitigate any negative impact

CyberSafety: Deradicalizing YouTube

- Investigate how YouTube's recommendation algorithm plays a role in online radicalization via surfacing extreme content
  - Prevalence of religiously intolerant Arabic YouTube videos, the tendency of the platform to recommend such videos, and how these recommendations are affected by demographics and watch history.
  - Used YouTube's API to collect data
  - Using crowdworkers, acquired annotations for a subset of videos to identify the ones promoting religious hate along with the targeted religious group(s)
  - For each video, collected its top four recommendations going five levels deep
  - Effect of personalization: carefully crafted eight different user profiles, each with a distinctive set of personal attributes

CyberSafety: Snapchat as a Lens on Public health

- Investigate how exposure to food snaps impacts the eating habits of the users
  - Collected Snapchat snaps from users in three different countries
  - Identified food-related snaps
  - Conducted user studies

CyberSafety: Hate speech in Arabic social media

- Religious hatred is a serious problem on Arabic social media (Twitter, YouTube)
- Goals: (1) Quantify and characterize religious hate speech on Arabic Twitter space; (2) develop classifiers to automatically detect religious hate speech in Arabic social media; and (3) To develop tools to detect bots involved in spreading religious hate

- Collected a large dataset of Arabic tweets and analyzed for religious hate content
- Developed classifiers to detect religious hate in Arabic Twitter
- Developed tools to detect bots in Arabic twitter

CyberSafety: Content Deletion and Moderation on Social Media Platforms

- Social media platforms strive to moderate their content by censoring, demonetizing and/or removing posts that allegedly violate their community guidelines
- Such practices could be met with resentment, anger, and in some cases, violence by users, especially if they are seen as unjust
- Users also sometimes delete their posted content for various reasons, one of which could be regret
- Goal: To understand the characteristics of posts that get deleted, and an ability to predict deletion before posting contents on these platforms to help reduce any aftermath of unfortunate consequences

- Monitored about 74,000 YouTube videos
- ~18% were deleted with in first seven days
- Done a detailed analysis of the features that (1) distinguish deleted videos from undeleted ones, (2) distinguish videos deleted by YouTube from videos deleted by users
- Developed classifiers to predict videos that will likely get deleted

- Contributors
  - Nuha Albadi, Maram Kurdi

Democracy and Technology

Democracy and Technology: Impact of technology on our democratic process

- A serious mismatch is gradually developing between two seemingly unrelated issues:
  - The penetration of science and technology into all aspects of our life, and
  - Democracy, as practiced throughout the free world
- Could these technologies endanger the foundations of liberal democracy?
- Goal: To strengthen democracy through technology

"The FBI's work was taken over in May 2017 by former FBI director Robert Mueller, who led a Special Counsel

ELECTION 2016 INTERNET AND NEW MEDIA RUSSIA

New Studies Show Pundits Are Wrong About Russian Social-Media Involvement in US Politics

Far from being a sophisticated propaganda campaign, it was small, amateurish, and mostly unrelated to the 2016 election.

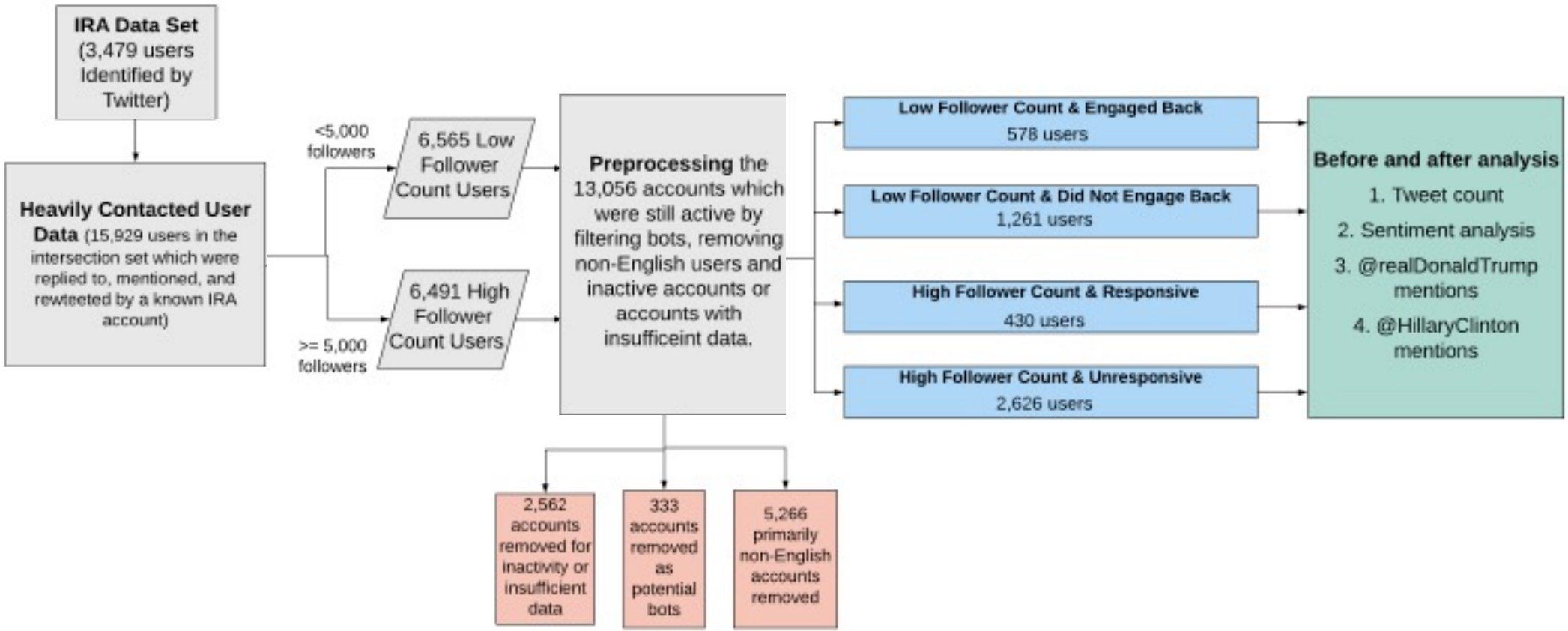
By Aaron Maté

DECEMBER 28, 2018

associated Americans, on unrelated charges." (Wikipedia entry for Russian Interference in Elections)

Current Project

- Evaluate impact of Internet Research Agency (IRA) behavior on Twitter users in the time before the 2016 U.S Presidential Elections


IRA Data Set (3,479 users Identified by Twitter)
Heavily Contacted User Data (15,929 users in the intersection set which were replied to, mentioned, and rewteeted by a known IRA account)
<5,000 followers
>= 5,000 followers
6,565 Low Follower Count Users
6,491 High Follower Count Users
Preprocessing the 13,056 accounts which were still active by filtering bots, removing non-English users and inactive accounts or accounts with insufficeint data.
2,562 accounts removed for inactivity or insufficient data
333 accounts removed as potential bots
5,266 primarily non-English accounts removed
Low Follower Count & Engaged Back
578 users
Low Follower Count & Did Not Engage Back
1,261 users
High Follower Count & Responsive
430 users
High Follower Count & Unresponsive
2,626 users
Before and after analysis
1. Tweet count
2. Sentiment analysis
3. @realDonaldTrump mentions
4. @HillaryClinton mentions

Before and After Analysis

- Increased monthly tweet activity for users that interacted with IRA
- Increase in the negativity of the sentiments in users that interacted with IRA
- Increased mentions of @RealDonaldTrump and @HillaryClinton in users that interacted with IRA
- Random baseline shows the changes are not generalizable to the rest of Twitter population

Democracy and Technology: Other projects

- Characterization of Toxicity Across Social Media Platforms
- Analyzing Behavioral Changes of Twitter Users After Exposure to Misinformation
- Understanding How Readers De- termine the Legitimacy of Online News Articles in the Era of Fake News

- Contributors
  - Rick Han, Tamara Lehman, Christine Lv
  - Jason Shuo Zhang
  - Rhett Hanscom, Yichen Wang
  - Upasana Dutta, Srihaasa Pidikiti

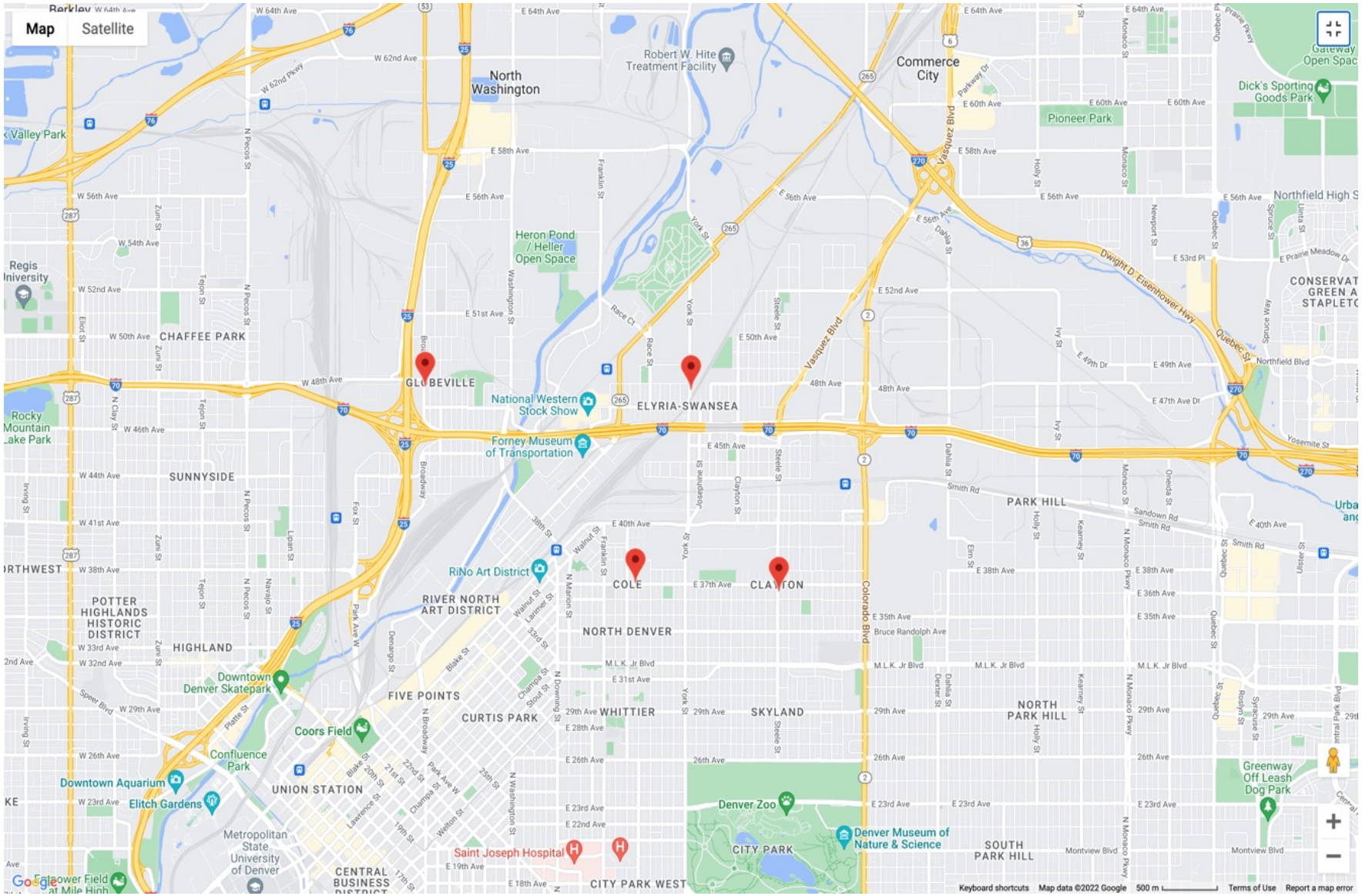
Socio-Technical Systems

Socio-Technical Systems: Introduction

- Communities in the US and around the world are entering a new era of transformation in which residents and their surrounding environments are increasingly connected through rapidly-changing intelligent technologies
- A socio-technical system refers to the interrelatedness of social and technical aspects of a community
- This interaction of social and technical factors creates the conditions that are beneficial to the community
- Research Goal: To exploit this intelligent technology now accessible to the end users to improve their health and well-being

Empowering Environmental Justice Communities with Smart and Connected Technology: Air and Noise Pollution, Wellbeing, and Social Relations in Times of Disruption

- To study two planned built environment disruptions in Denver, the C70 project and the NWC redevelopment
  - The Central 70 project (C70) is a 10-mile stretch of the I-70 interstate through northeast Denver where the interstate is being widened, an underground viaduct removed, and a section lowered
  - The National Western Center (NWC) redevelopment is doubling the complex footprint and land acquisition
- Three affected communities
  - Globeville, Elyria-Swansea, and Cole
  - Low socio-economic status, high unemployment, less than high school education, mostly Hispanic
  - A long legacy of environmental contamination


Map
Satellite
North Washington
Robert W. Hite Treatment Facility
Commerce City
Pioneer Park
Dick's Sporting Goods Park
Heron Pond / Heller Open Space
Regis University
CHAFFEE PARK
GLOBEVILLE
National Western Stock Show
ELYRIA-SWANSEA
Forney Museum of Transportation
Rocky Mountain Lake Park
SUNNYSIDE
RiNo Art District
RIVER NORTH ART DISTRICT
COLE
CLAYTON
PARK HILL
POTTER HIGHLANDS HISTORIC DISTRICT
HIGHLAND
NORTH DENVER
Downtown Denver Skatepark
FIVE POINTS
CURTIS PARK
WHITTIER
SKYLAND
NORTH PARK HILL
Coors Field
Confluence Park
Downtown Aquarium
Elitch Gardens
UNION STATION
Metropolitan State University of Denver
Saint Joseph Hospital
CENTRAL BUSINESS DISTRICT
CITY PARK WEST
Denver Zoo
CITY PARK
Denver Museum of Nature & Science
SOUTH PARK HILL
Greenway Off Leash Dog Park
Dwight D. Eisenhower Hwy
Vasquez Blvd
Colorado Blvd
Quebec St
Keyboard shortcuts
Map data ©2022 Google
500 m
Terms of Use
Report a map error

- Current Project
  - To build a socio-technical system comprised of environment sensors, smartphone platforms, and a data analytics server equipped with predictive modeling and visualization to
    1. understand the personal environment (air and noise pollution), individual wellbeing, and social relations of environmental justice communities affected by a major planned disruption in their built environment
    2. mitigate negative impacts of a planned disruption, and
    3. equip policy and decision makers with information in advance about potential negative impacts of upcoming disruptions to help them plan appropriate safeguards.

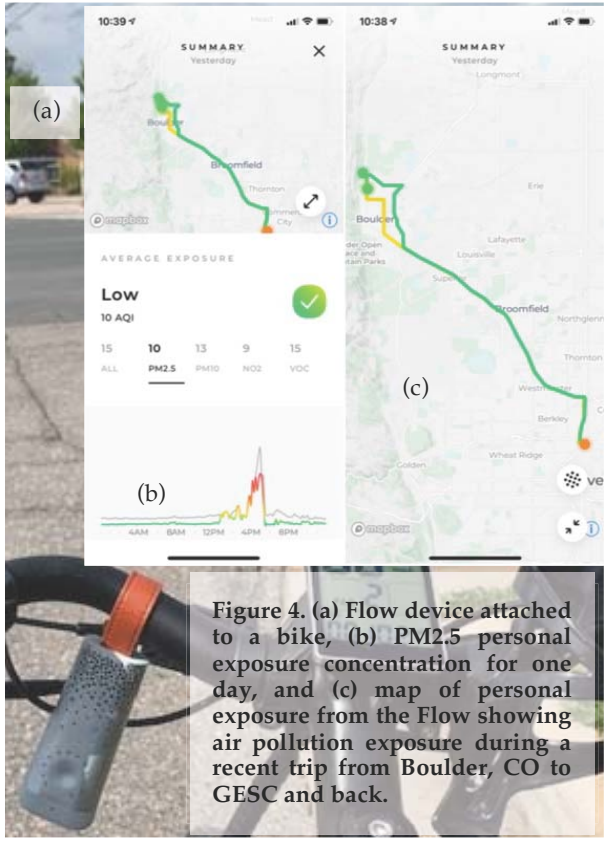
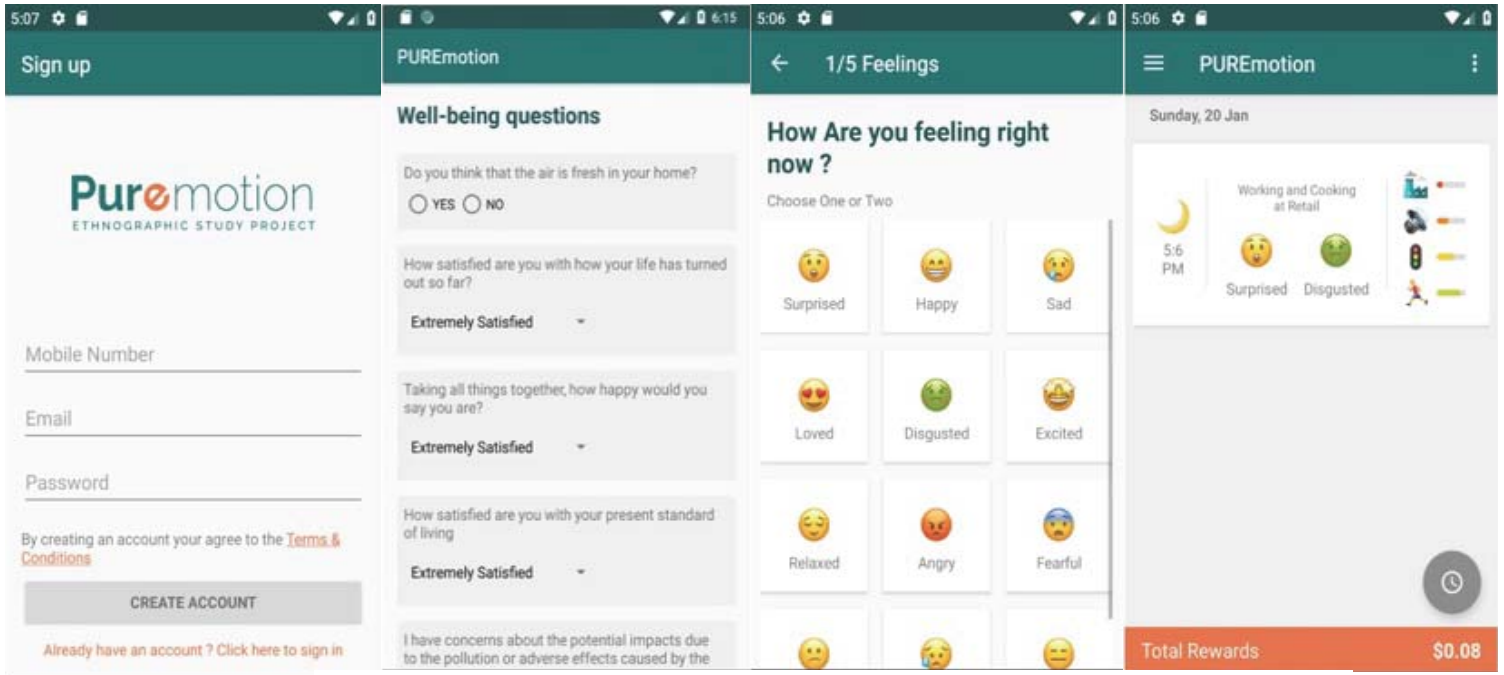
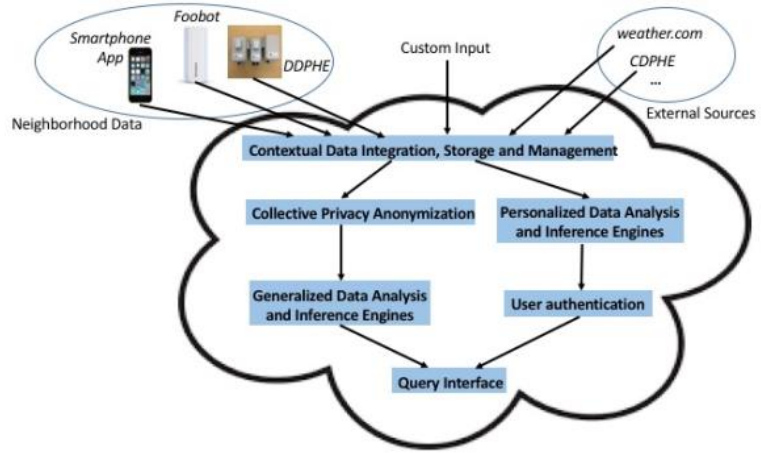


Figure 4. (a) Flow device attached to a bike, (b) PM2.5 personal exposure concentration for one day, and (c) map of personal exposure from the Flow showing air pollution exposure during a recent trip from Boulder, CO to GESC and back.





- Three Smartphone Apps
  - PureMotion
  - PureConnect
  - PureNav
- Personal air monitors
- Deployment over four cohorts
  - Winter 2021, Summer 2022, Winter 2022, Summer 2023

- Contributors
  - Shelly Miller, Esther Sullivan, Nicholas Clements
  - Omar Hammad, Md. Rezwanur Rahman, Gopala Kanugo, Neerab Pathipaka, Jacob McKinney

- I am looking for students interested in participating in any of these projects
  - Ph.D., MS thesis, MS independent study, Undergraduate thesis
- If you are interested

Email me: mishras@colorado.edu

Thank You!!!