CAREER: A Holistic Context-based Approach for Security and Privacy in the Era of Ubiquitous Sensing and Computing

PI: Murtuza Jadliwala, University of Texas at San Antonio

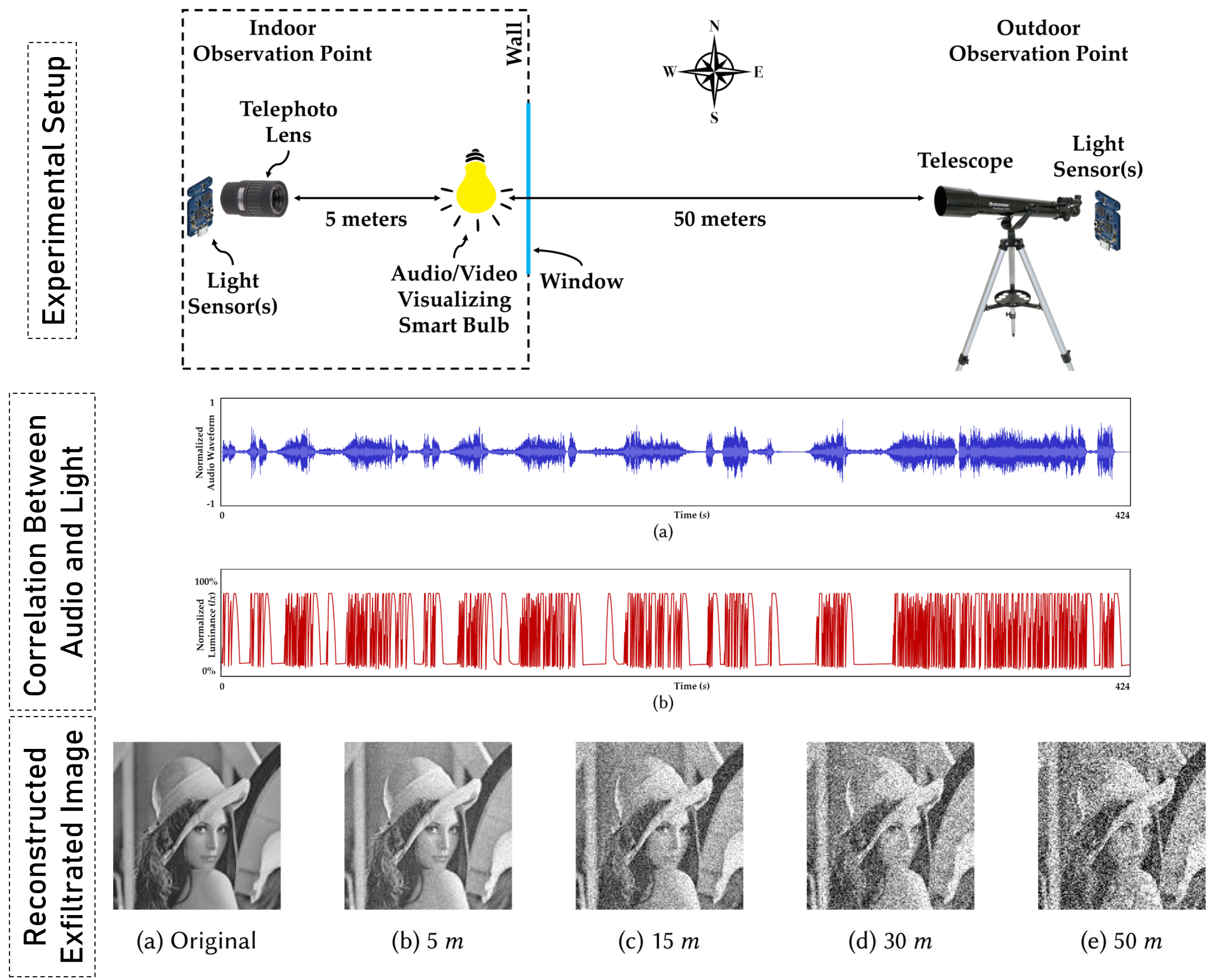
https://sprite.utsa.edu/people/mjadliwala/

Research Goals

- To uncover new security & privacy risks in modern ubiquitous sensing and computing systems, comprising of a disparate set of sensors/actuators and end-users with different privacy preferences.
- To enable secure and privacy-preserving sensor access control by exposing fine-grained and holistic user-context and harnessing it at various operational (device & network) levels.

Security and Privacy Risks (On-going)

Information Leakage via Smart Lights [4]

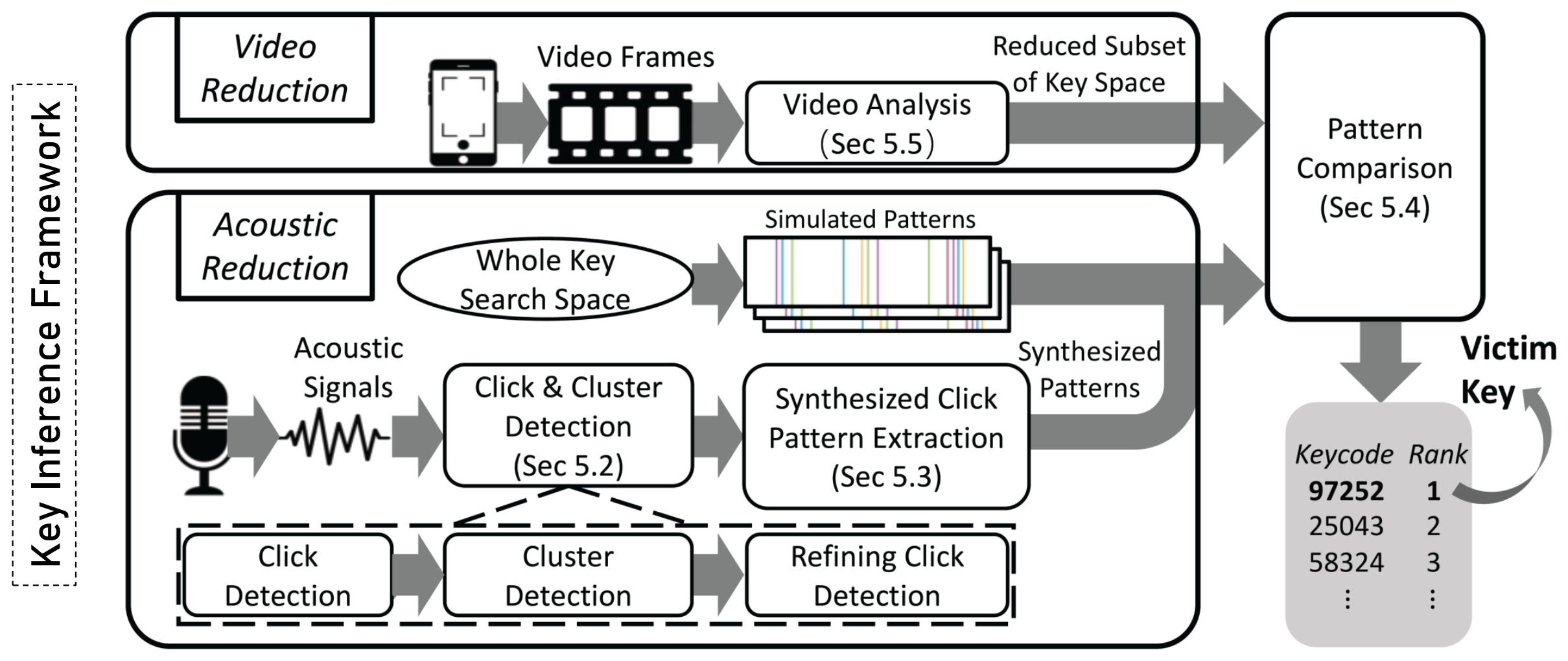

Experimental Setup
Indoor Observation Point
Wall
Telephoto Lens
5 meters
Light Sensor(s)
Audio/Video Visualizing Smart Bulb
Window
N
W
E
S
50 meters
Outdoor Observation Point
Telescope
Light Sensor(s)
Correlation Between Audio and Light
Normalized Audio Waveform
1
-1
0
Time (s)
424
Normalized Luminance (lx)
100%
0%
Time (s)
Reconstructed Exfiltrated Image

(a)

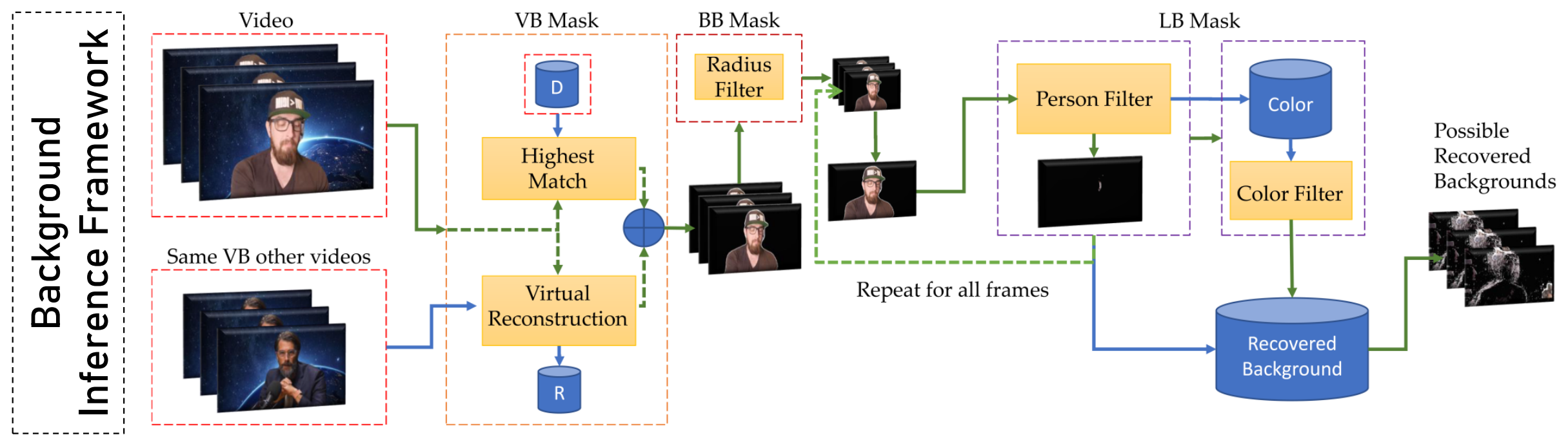
(b)

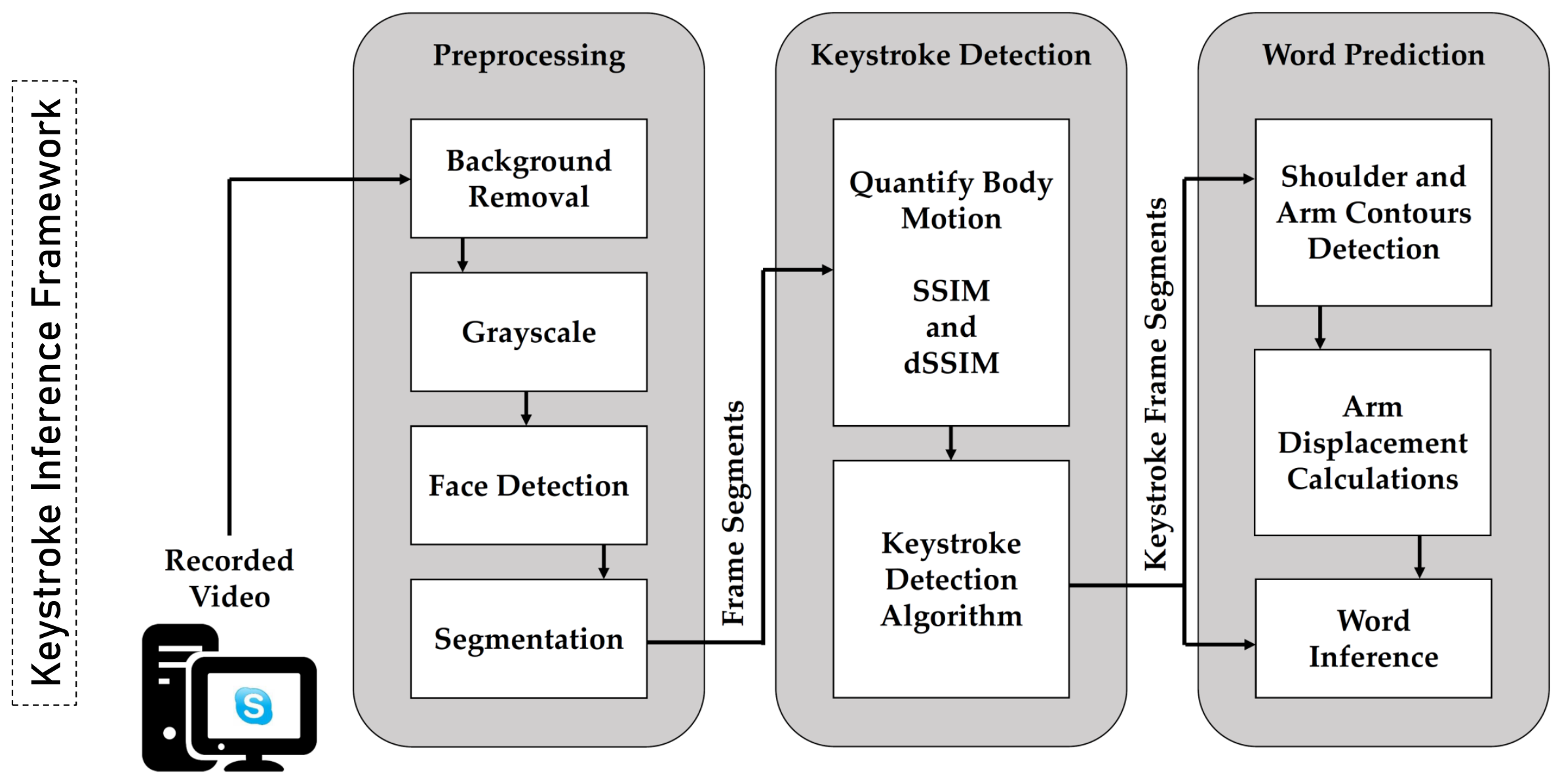
(a) Original (b) 5 m (c) 15 m (d) 30 m (e) 50 m

Physical Key Inference [2]



Information Leakage in Video Calls [1,3]



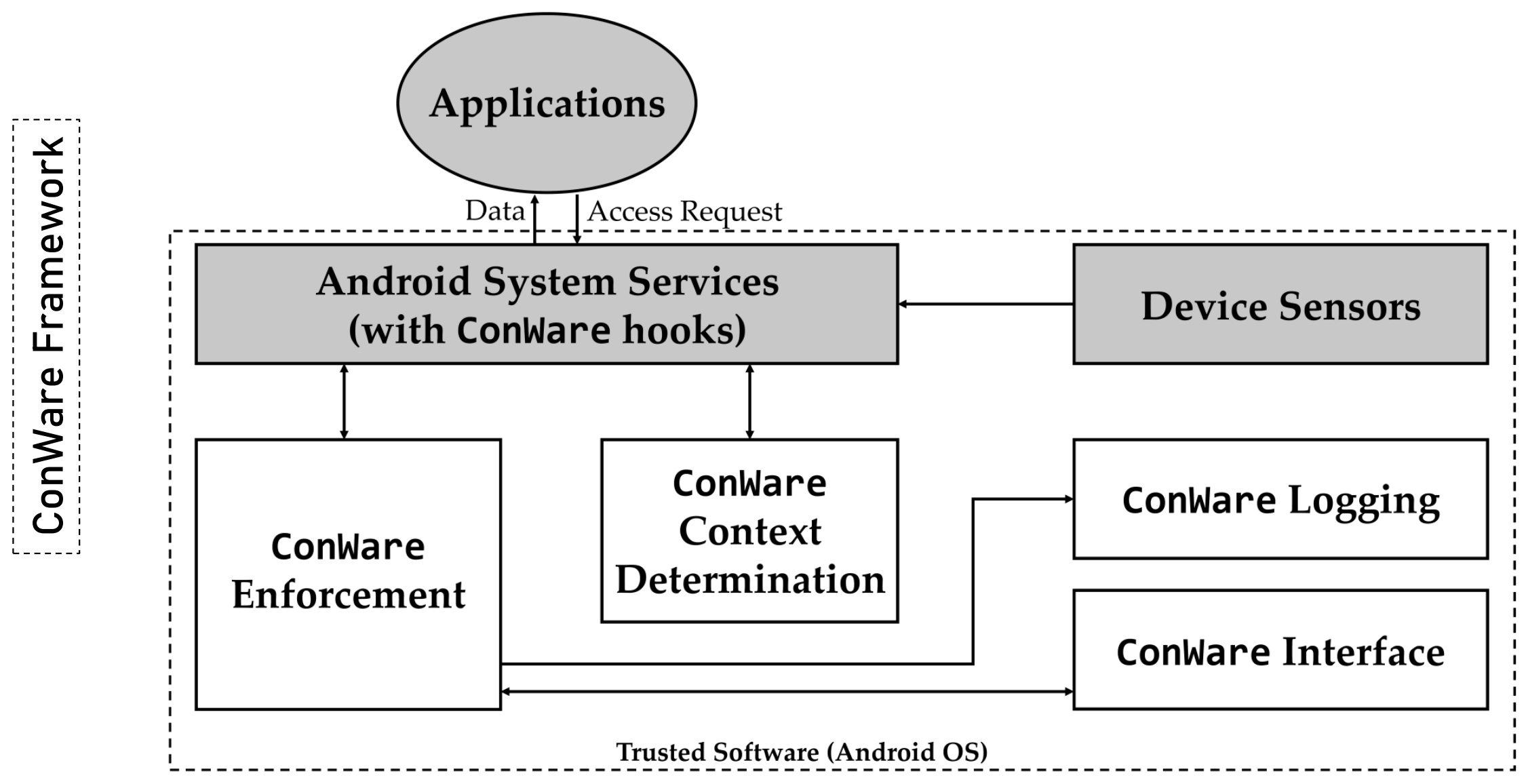


Related Publications:

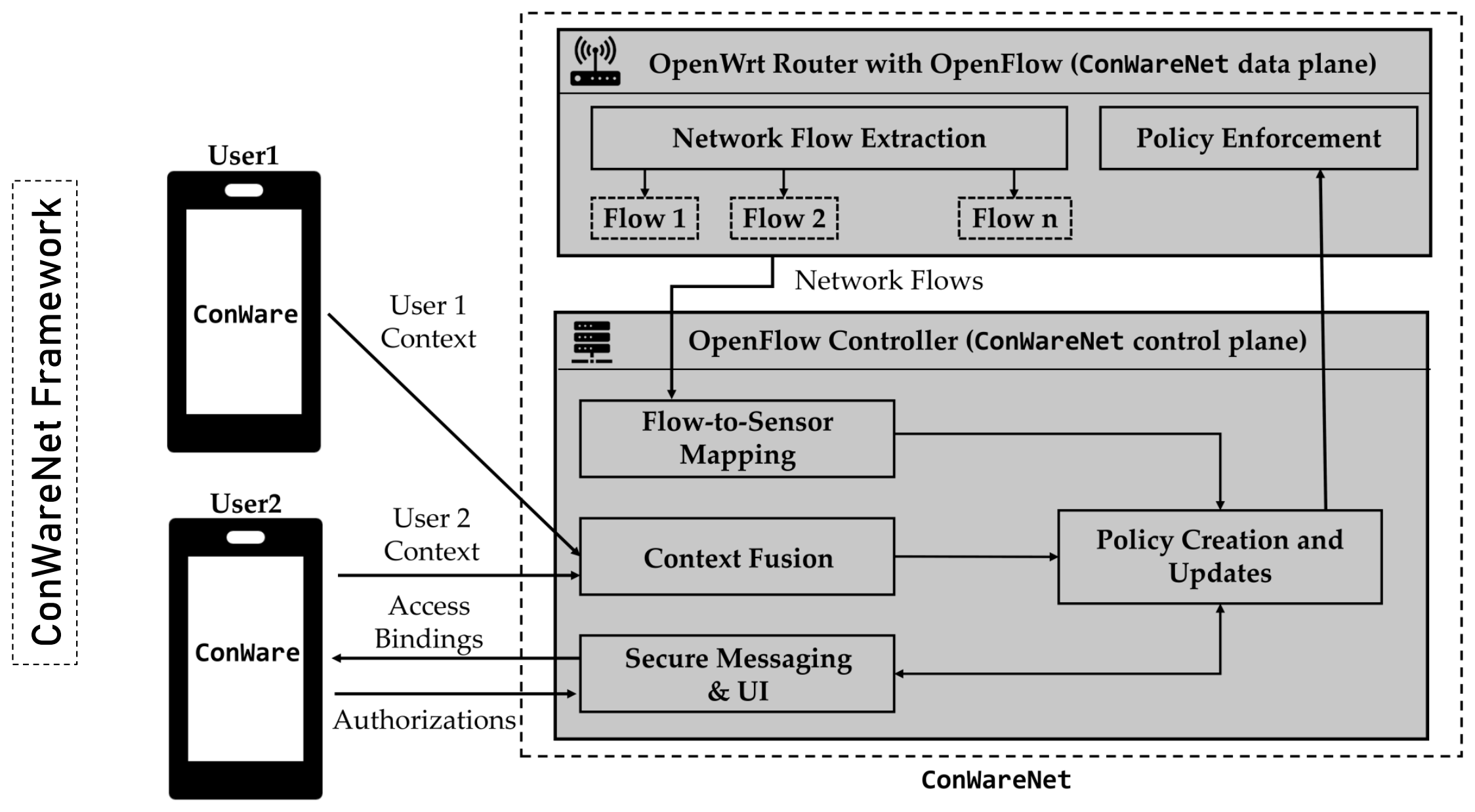
1. Mohd Sabra, Anindya Maiti, and Murtuza Jadliwala, "Background Buster: Peeking through Virtual Backgrounds in Online Video Calls", IEEE DSN, 2022.
2. Soundarya Ramesh, Xiao Rui, Anindya Maiti, Jong Taek Lee, Harini Ramprasad, Ananda Kumar, Murtuza Jadliwala, and Jun Han, "Acoustics to the Rescue: Physical Key Inference Attack Revisited", USENIX SECURITY, 2021.
3. Mohd Sabra, Anindya Maiti, and Murtuza Jadliwala, "Zoom on the Keystrokes: Exploiting Video Calls for Keystroke Inference Attacks", ISOC NDSS, 2021.
4. Anindya Maiti, and Murtuza Jadliwala, "Light Ears: Information Leakage via Smart Lights", ACM IMWUT (presented at ACM UbiComp), 2019.

Host and Network Based Protection (Future Work)

ConWare: Harness exposed user context at the device level.



ConWareNet: Harness exposed user context at the network level.



Adaptive Protection (Future Work)

- How to adapt the operation/functionality of ConWare and ConWareNet when new sensors, actuators, controllers and users join or leave the system?
  - Challenge: How to detect and resolve conflicts in existing policies and access bindings?
- How to make ConWare and ConWareNet robust against context misuse?
  - Challenge: How to effectively hide the exposed context from recipients who cannot authorize themselves?

Boarder Impacts (On-going and Future Work)

- Develop hands-on curriculum in mobile and IoT security at multiple levels (K-12, undergraduate, graduate).
- Community-focused educational summer camps, courses and training initiatives.
  - 1st Cyber Warriors Cybersecurity Summer Camp (2021)
    - One week camp from July 26-30, 2021, organized virtually
    - Attended by 8 students from San Antonio area high-schools, with several belonging to low-income & minority communities
  - 2nd Cyber Warriors Cybersecurity Summer Camp (2022)
    - https://sprite.utsa.edu/cyberwarrior22

The 5th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
June 1-2, 2022 | Arlington, Virginia

Award ID#: 1943351