Trusted Timing Services for Untrusted Cloud-Edge Systems

Fatima Anwar
fanwar@umass.edu
UMass Amherst

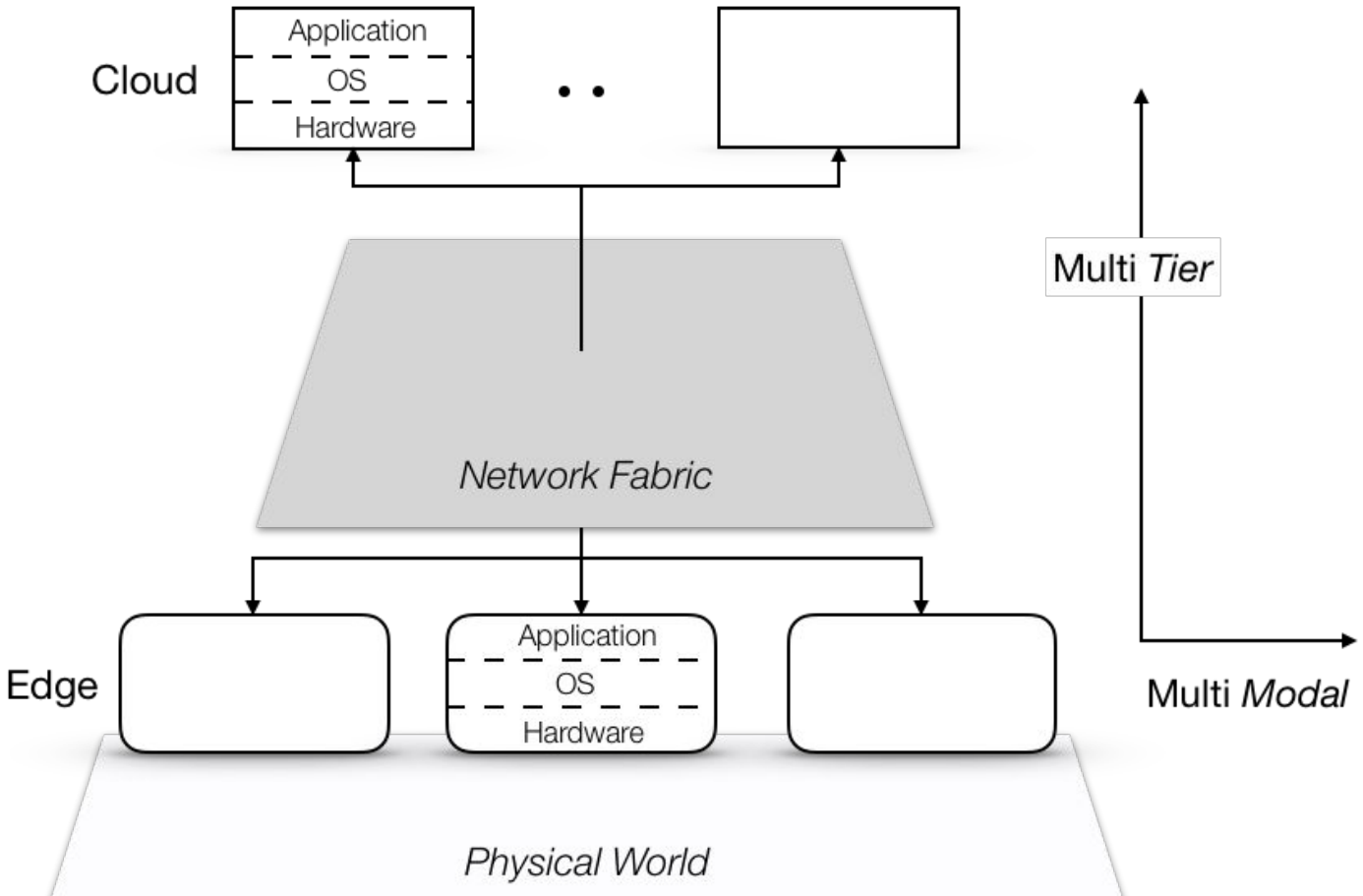
In collaboration with my PhD advisees:
Yasra Chandio, Adeel Nasrullah, Khotso Selialia, Momin Khan, Abdullah Soomro

Outline

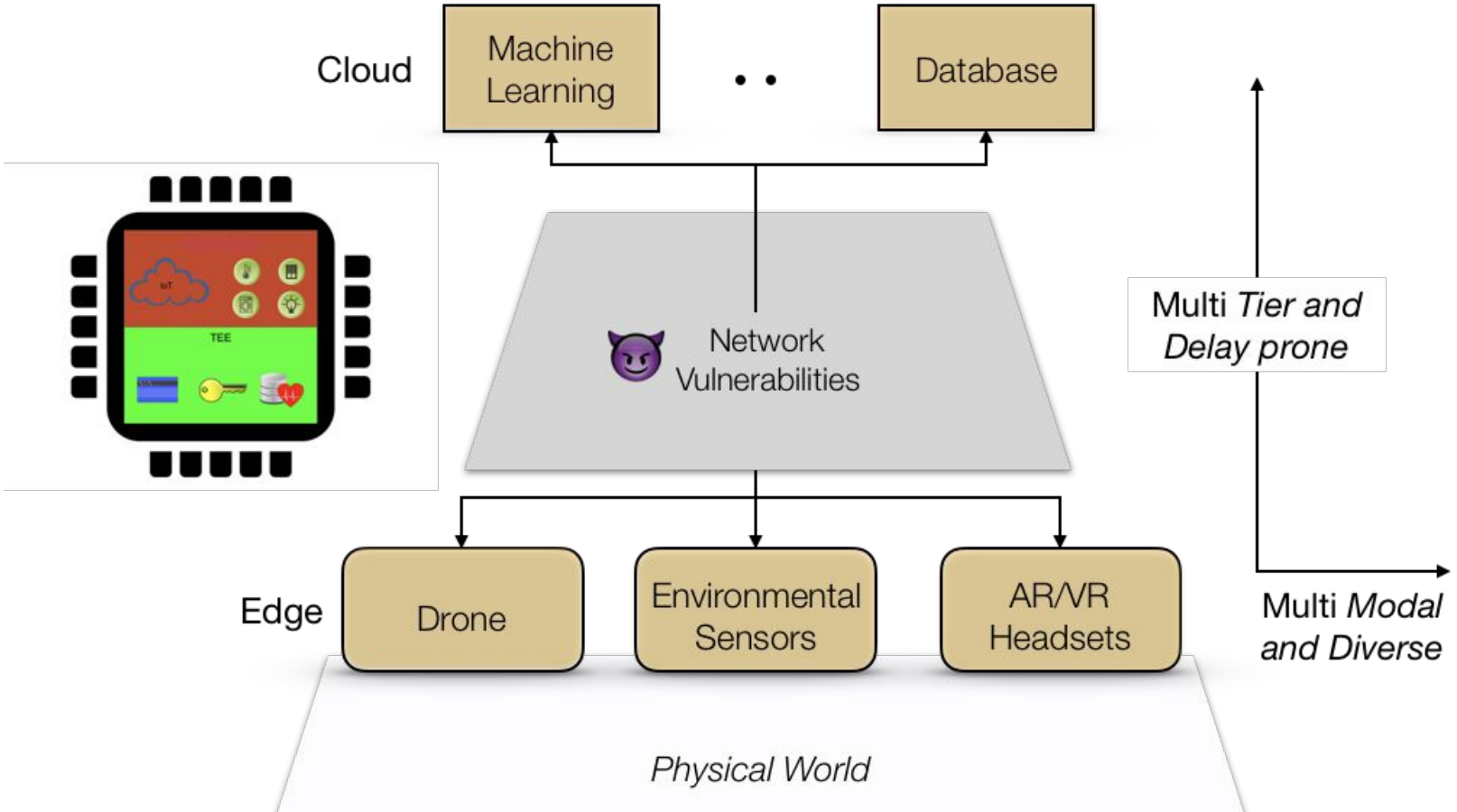
1. What are cloud-edge systems
2. Usage of System Services in cloud edge systems
    a. Timing, Tracking, Learning
3. Timing Vulnerabilities in System Services
4. Threat Model
5. Trusted Time Architecture

What are cloud-edge systems?

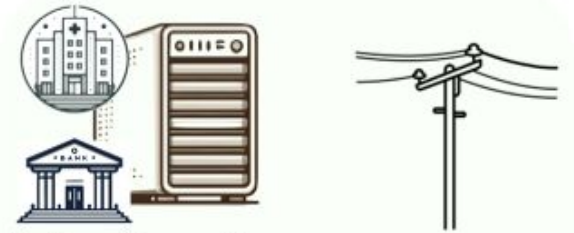
Networked Cloud-Edge System



Untrusted Cloud-Edge System



Usage of Timing Services



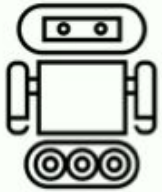
Online Security & Privacy

Smart Grid

Manufacturing

Infrastructure

GPS



Visual-Inertial Odometery

Driver Assistance

Navigation

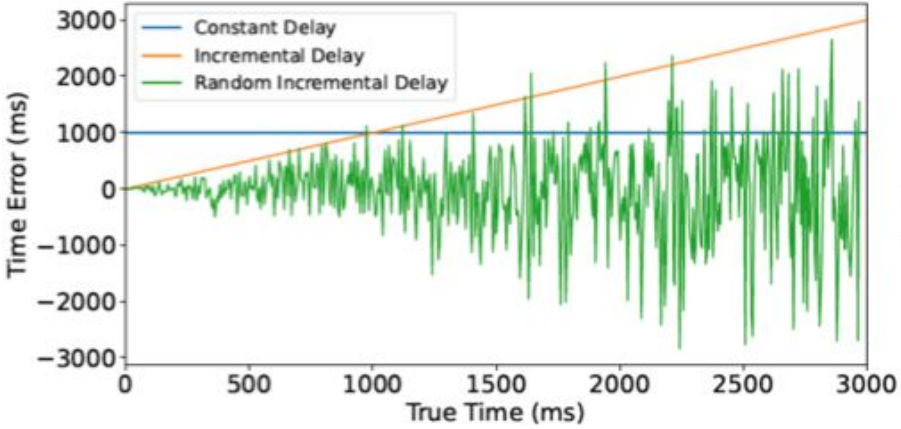
Fall Detection

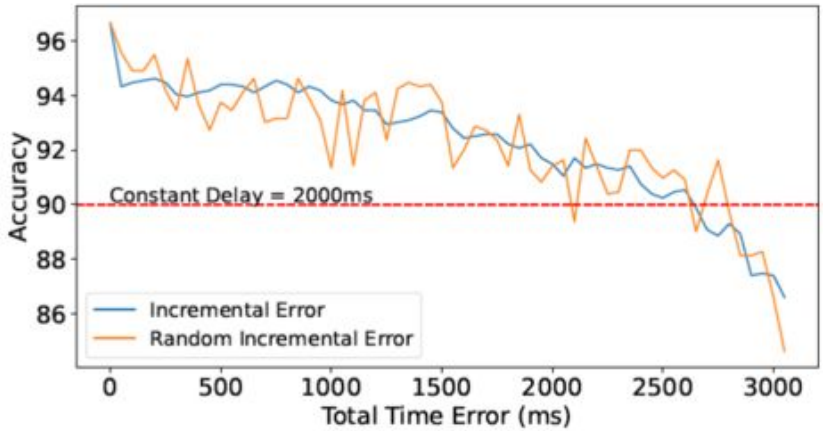
Muscle Fatigue Estimation

Environmental Conservation

Sensor Networks

Time Vulnerabilities in Timing Services





Time Error Accumulation

Accuracy Degradation of Multi-modal ML

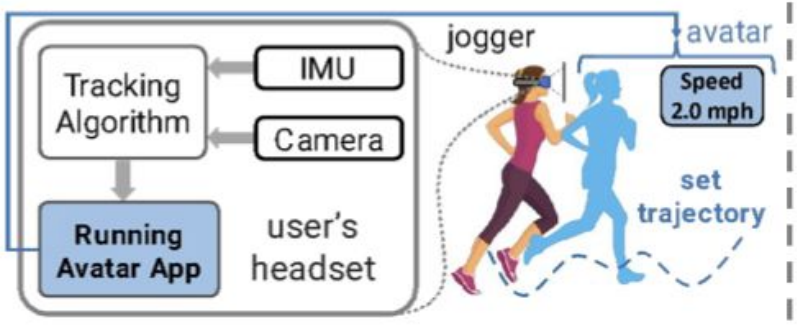
Malicious Time Error degrades system performance and may compromise human safety

Ref: Sandha, S. S., Noor, J., Anwar, F. M., & Srivastava, M. (2020, April). Time awareness in deep learning-based multimodal fusion across smartphone platforms. In 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI)

Usage of Tracking Services

Time Vulnerabilities in Tracking Services

Malicious Tracking disturbs actual human trajectory
and may compromise human safety

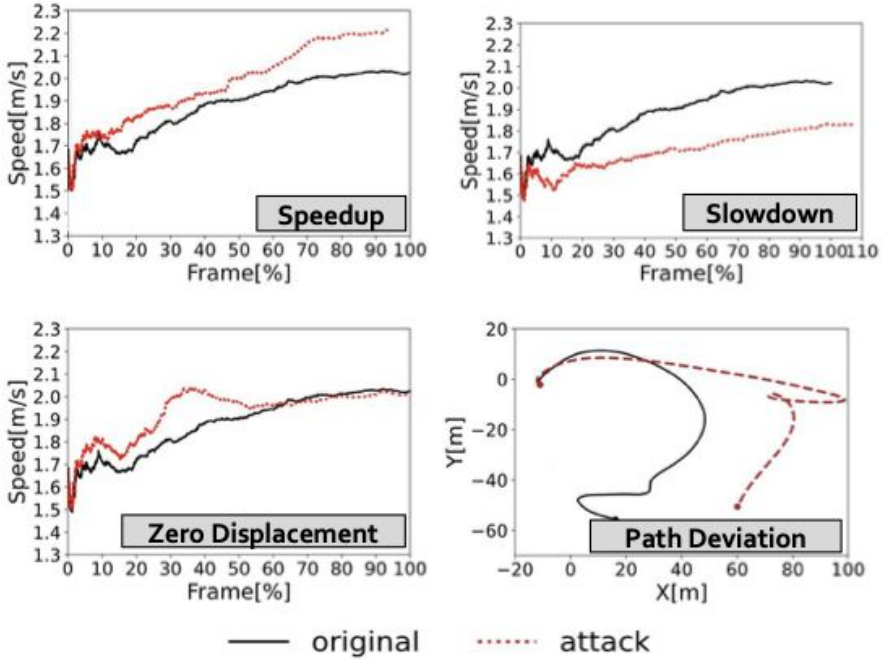


Jogging with a partner avatar

Ref: Chandio, Yasra, Noman Bashir, and Fatima M. Anwar. "Stealthy and Practical Multi-modal Attacks on Mixed Reality Tracking." 2024 IEEE International Conference on Artificial Intelligence and eXtended and Virtual Reality (AIxVR). IEEE, 2024.

Time Vulnerabilities in Tracking Services

Malicious Tracking disturbs actual human trajectory and may compromise human safety



Speedup Attack:
Application perceives user speedup and prompt user to walk slower

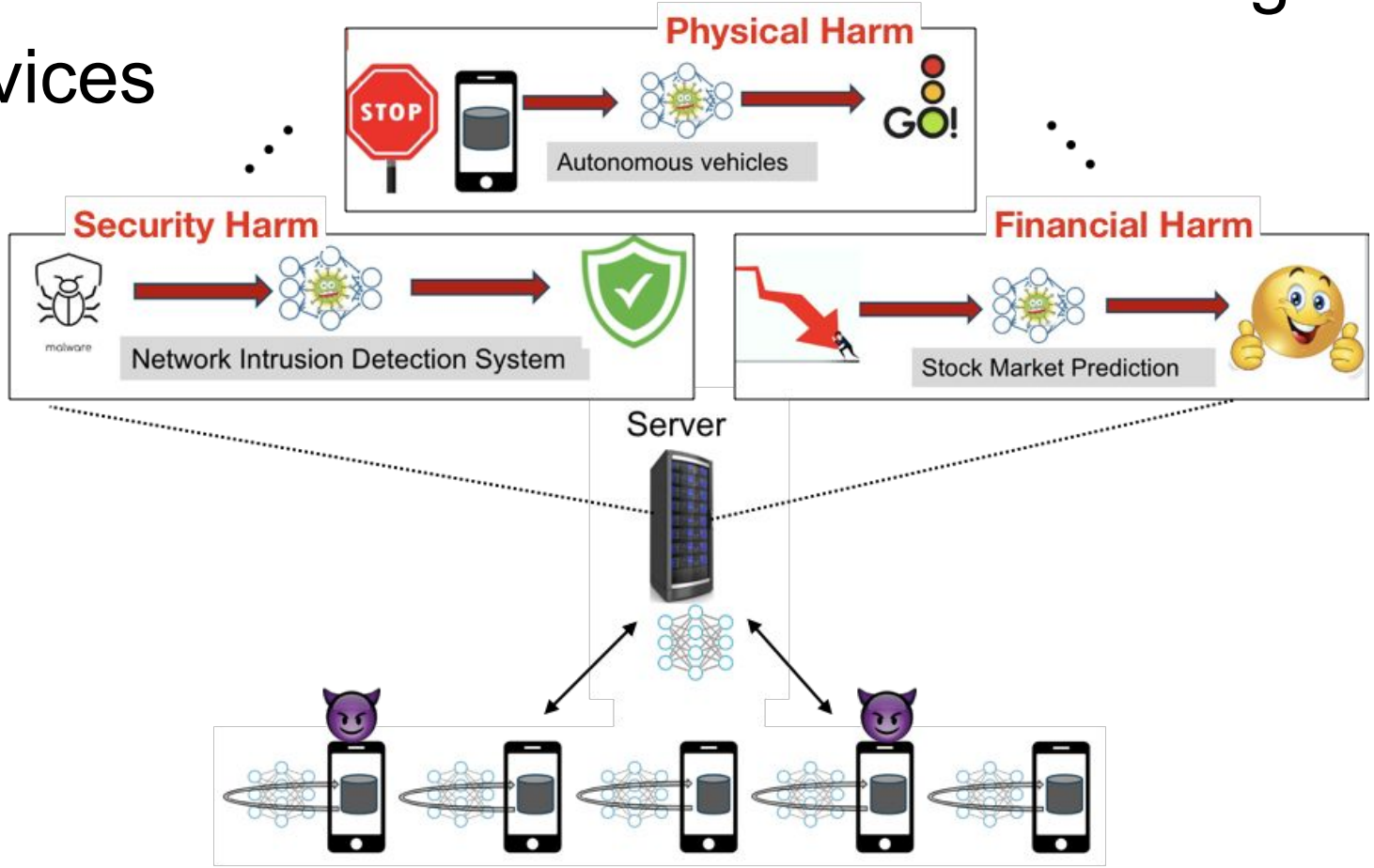
Slowdown Attack:
Application perceives user slowdown and prompt user to walk faster

Zero Displacement Attack:
User reaches the destination through a different path

Path Deviation Attack:
User is unable to reach the destination

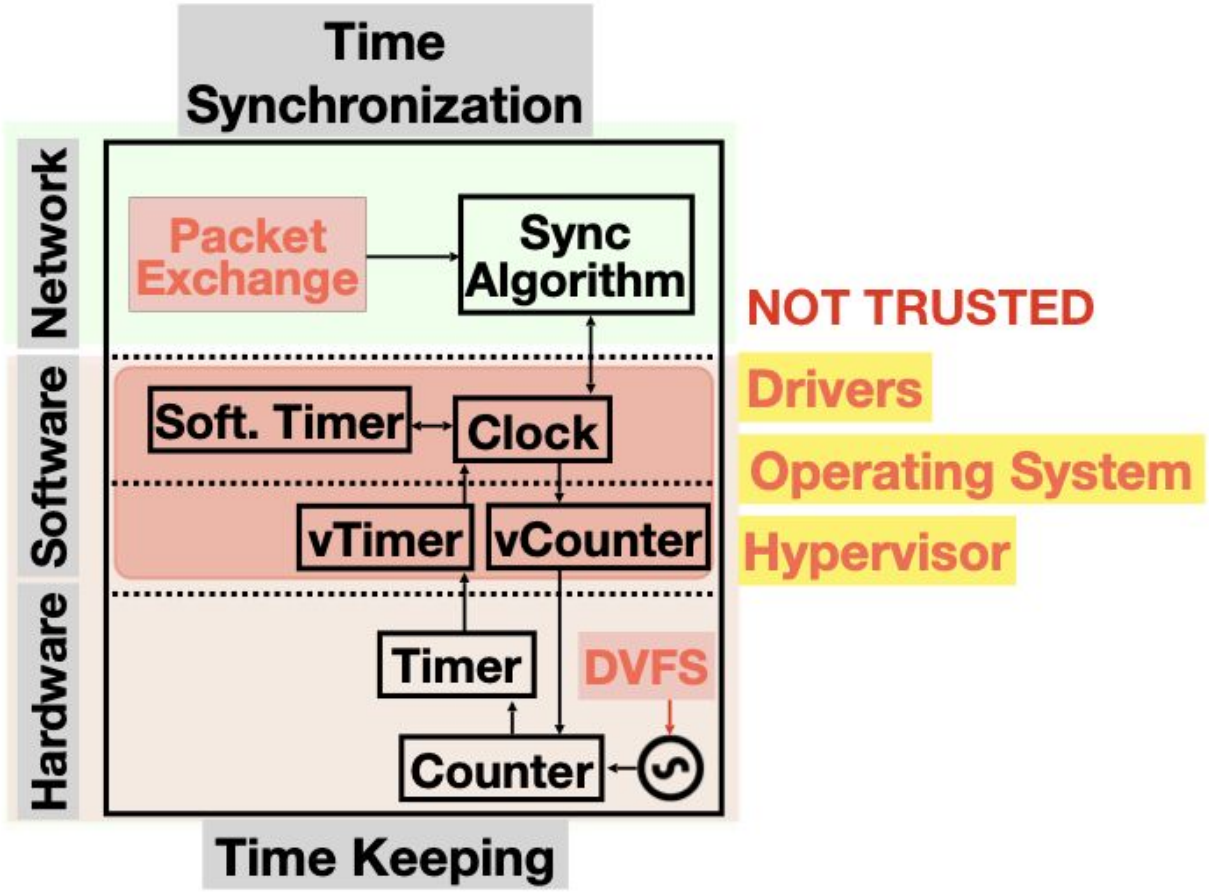
Ref: Chandio, Yasra, Noman Bashir, and Fatima M. Anwar. "Stealthy and Practical Multi-modal Attacks on Mixed Reality Tracking." 2024 IEEE International Conference on Artificial Intelligence and eXtended and Virtual Reality (AIxVR). IEEE, 2024.

Time Vulnerabilities in Distributed Learning Services



Ref: Momin Khan, Virat Shejwalkar, Amir Houmansadr, and Fatima M. Anwar. "On the pitfalls of security evaluation of robust federated learning." The 2023 IEEE Security and Privacy Workshops (SPW). 2023.

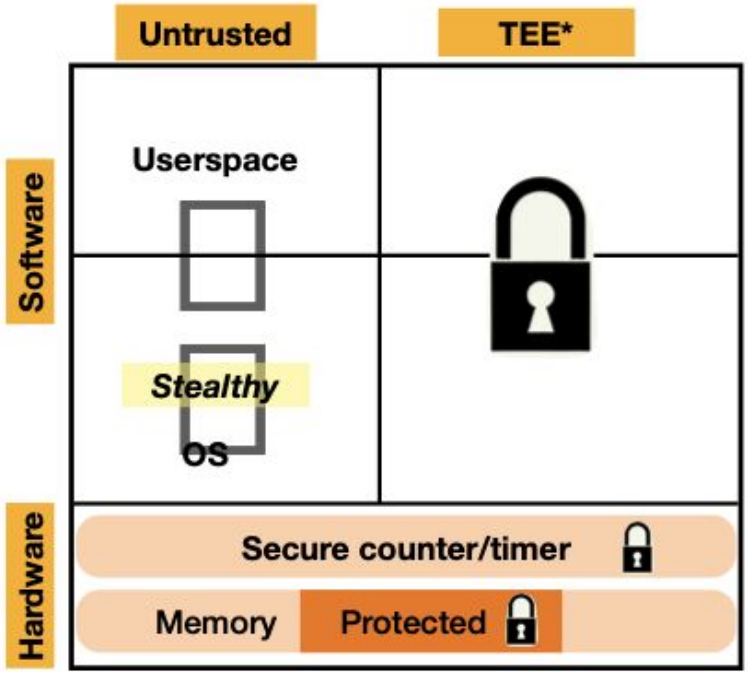
Why can’t we trust time?



Threat Model

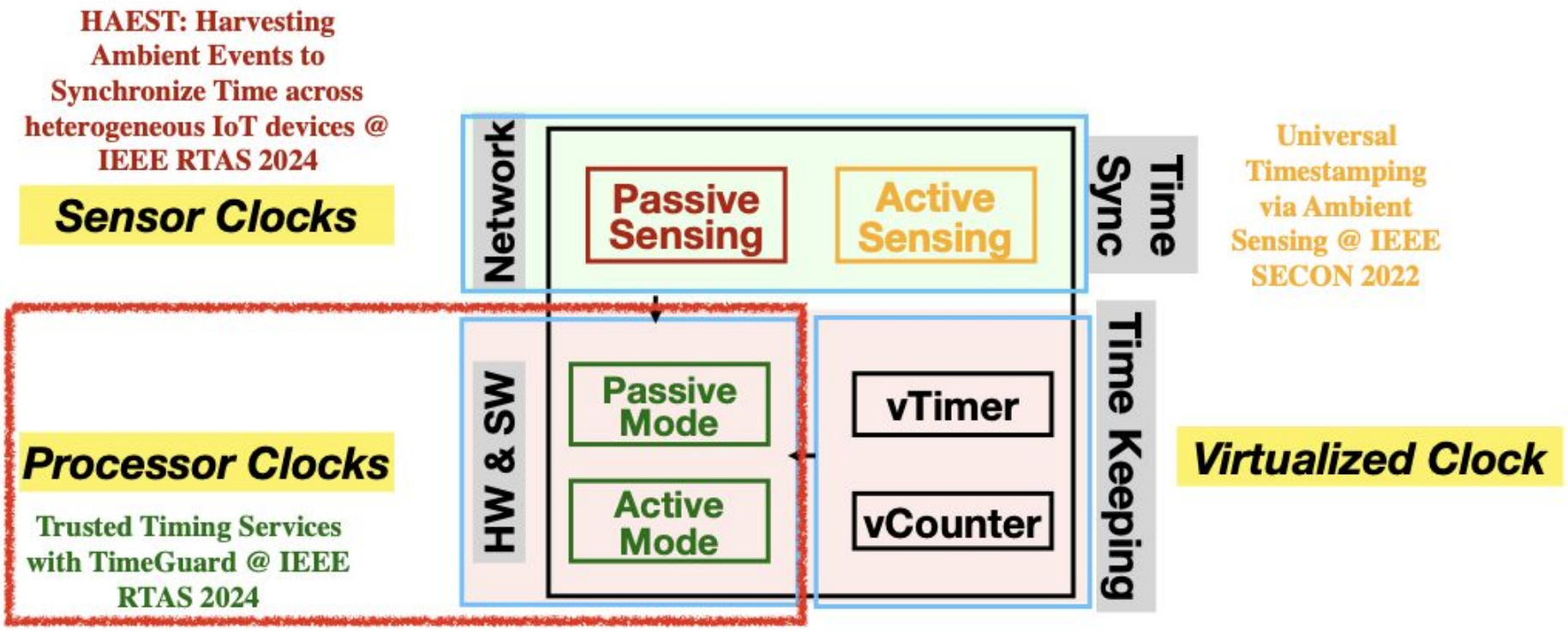
*Trusted Execution Environment
- ARM Trustzone
- RISC-V Keystone
- Intel SMM/SGX

- ✓ Privileged Code Execution
- ✓ Hijack Exception Handlers
- ✓ Program Timer Interrupts
- ✓ Profile target programs to collect statistics e.g. use of system_call



Redesign Timing Service:
Trusted Time Architecture

Trusted Time Architecture



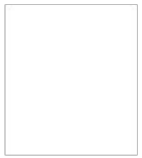
* This work is supported by my CAREER grant,"Secure Timing Architecture for Untrusted Edge Systems"

Available to applications inside and outside secure enclaves

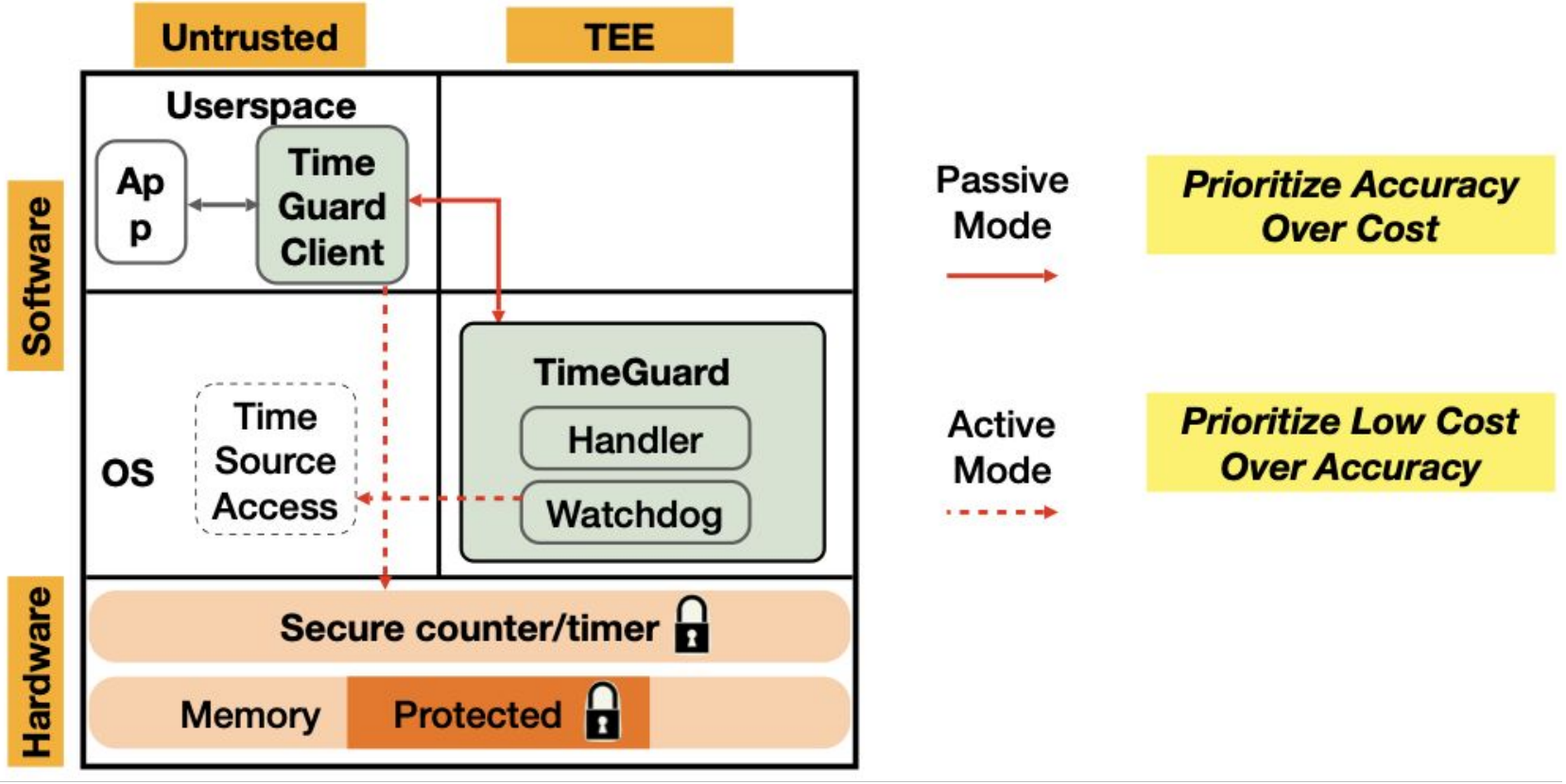
How to build a *system-wide trusted time service* hardened against *privileged adversaries* with an *optimal security vs cost trade-off* ?

e.g. compromised OS

cost is proportional to the time accuracy guarantee



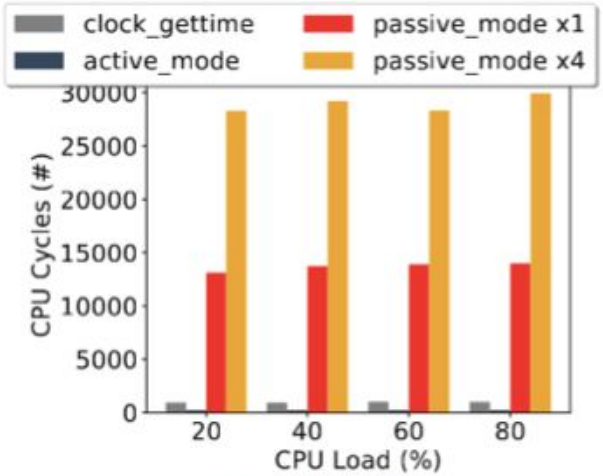
Processor Clock - Big Picture



Ref: Nasrullah, Adeel, and Fatima M. Anwar. "Trusted Timing Services with Timeguard." *30th Real-Time and Embedded Technology and Applications Symposium (RTAS)*. IEEE, 2024.

Cost v/s Accuracy

Cost of timestamping APIs

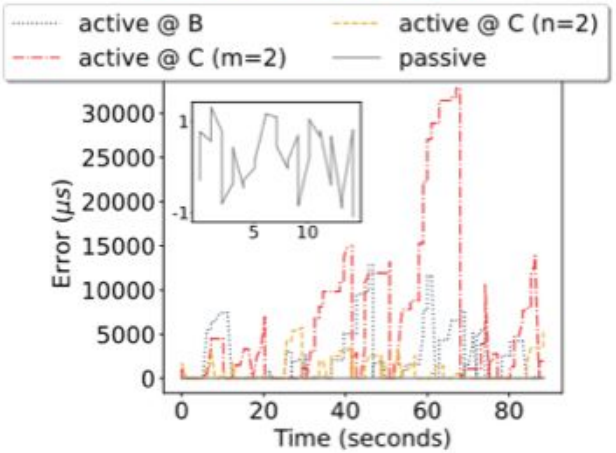


Key Result

*Active mode is **x20 less expensive** than linux **clock_gettime.***

*Passive mode is **x25 more expensive** than the linux **clock_gettime.***

Average time error



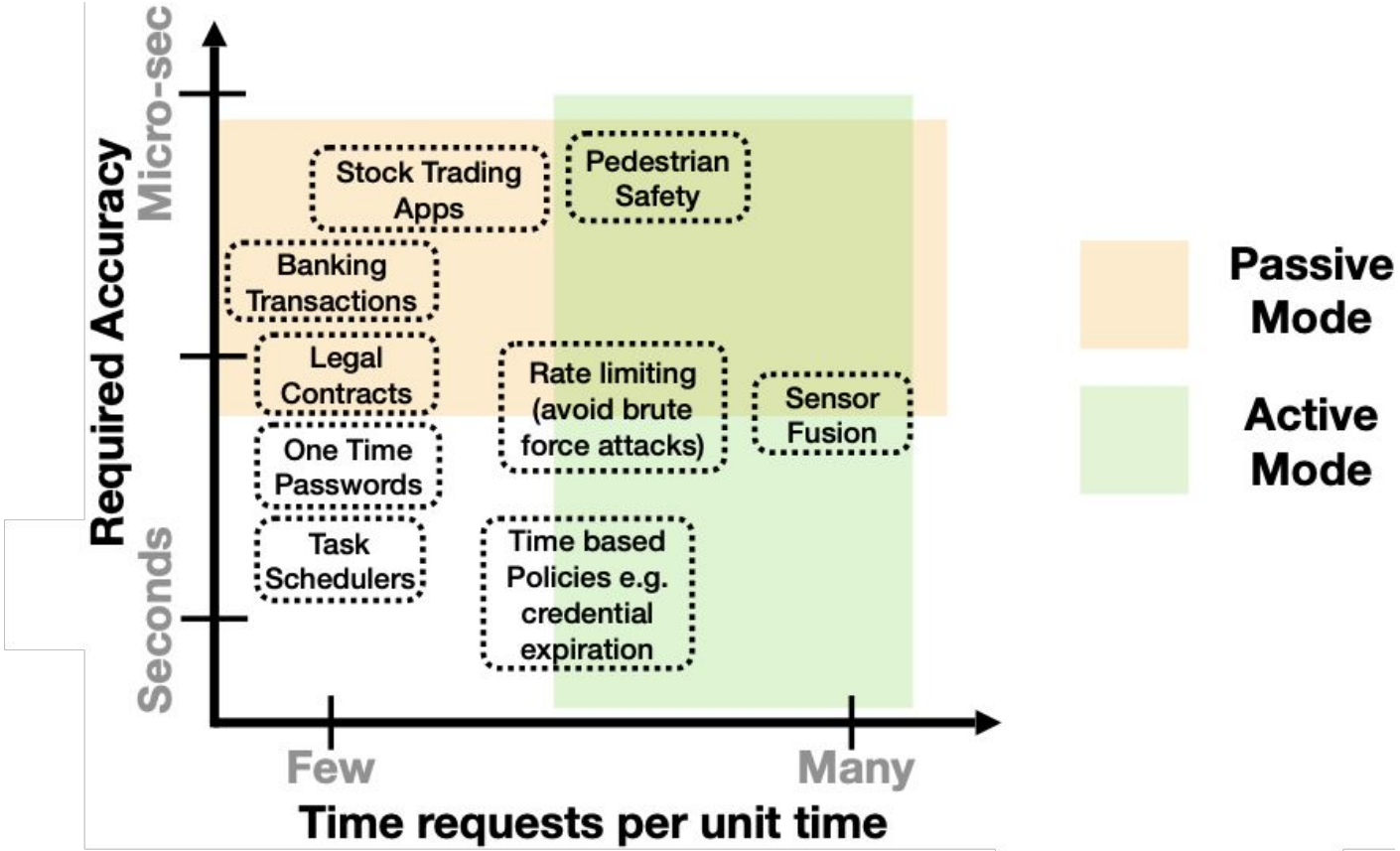
Key Result

*Active mode provides time **accurate upto a few milliseconds.***

*Passive mode provides time **accurate upto few microseconds.***

Ref: Nasrullah, Adeel, and Fatima M. Anwar. "Trusted Timing Services with Timeguard." *30th Real-Time and Embedded Technology and Applications Symposium (RTAS)*. IEEE, 2024.

Usage of Passive v/s Active Mode



Ref: Nasrullah, Adeel, and Fatima M. Anwar. "Trusted Timing Services with Timeguard." *30th Real-Time and Embedded Technology and Applications Symposium (RTAS)*. IEEE, 2024.

Summary

1. Introduced cloud-edge systems with examples
2. Shown usage of System Services such as timing, tracking, and learning in cloud edge systems
3. Demonstrated Timing Vulnerabilities in System Services
4. Demonstrated a processor clock in Trusted Time Architecture and shown its application scope