Poster: Leveraging In-Sensor Computing to Preserve Privacy in Remote Health Monitoring

Mashrafi Kajol, Nishanth Chennagouni
University of New Hampshire

Andrew Lu
Oyster River High School

Wei Lu
Keene State College

Dean Sullivan and Qiaoyan Yu
University of New Hampshire

I. Introduction

The increasing availability of sensor technology enables trending progress in cloud-based Electronic Health Records (EHR) systems. The success of cloud-based EHR (e.g., Fig. 1) not only improves patient diagnosis speed but also reduces the workload of the hospital staff [1]. Unfortunately, the current cloud-based EHR suffers from cyberattacks [2], harming the benefits of users, diagnosis parties, healthcare providers, and EHR enterprises. Among different types of breaches in health-monitoring applications, hacking, or Information technology (IT) incidents increased from 4.02% in 2010 to 43.44% in 2018 [3]. Interestingly, the rate of incidents that happened through laptops declined from 24.12% in 2020 to 4.64% in 2018 [3]. Increasing attacks happen at edge devices, which have limited limitation computation power budgeted for security measures. Several factors increase the risk of edge device manipulation [4] and privacy breaches [5]. Health Insurance Portability and Accountability Act of 1996 (HIPAA) primarily protects medical data privacy. However, many daily use devices and applications are outside the scope of HIPAA protections [6]. Thus, it is imperative to address the security and privacy of health-monitoring sensors, and communication channels between sensors to EHR clouds.

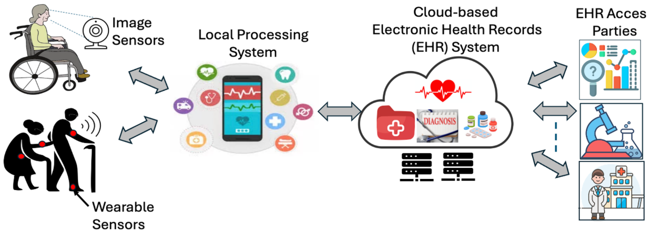


Fig. 1. Cloud-based Electronic Health Records (EHR) system.

II. Proposed Method

A. Method Overview

The communication channel from health-monitoring edge devices to cloud servers is vulnerable to information leakage. We propose to use In-Sensor Computing (ISC) to address the increasing concerns on the privacy and security of edge devices while minimizing the latency and energy consumption in sensory data transmission, analog-to-digital conversion (ADC), and data pre-processing. In-Sensor Computing (ISC) emerges as a new computation paradigm [7], [8]. Sensing units in an ISC do not only sense the target surroundings but also process data at the point of collection, rather than requiring extensive data transfer [7]. Different than the traditional wearable sensor and near-sensor computing architecture, we will design in-sensor computing architecture to simultaneously preserve sensor data privacy and minimize the size of sensor data while maintaining biometric features. Some sensing materials inherently have some computation power, the essence of which is a desired processing function implemented by leveraging specific material/device mechanisms. Different than traditional sensor system [9], near-sensor computing [10], we propose to integrate sensing material *(Sm)* and basic computation unit *(C)* into a single chip to perform preliminary data processing before readout and ADC, as shown in Fig. 2(c). The array of computing circuits can be configured via the built-in interface *ISC-Config* to extract the biometric features interested in continuous real-time monitoring applications.

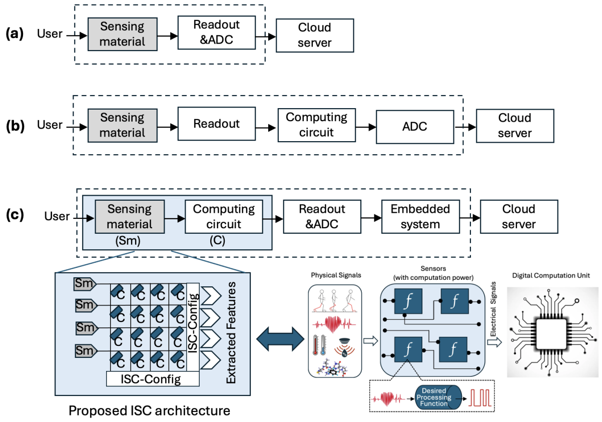


Fig. 2. Difference between existing sensor systems and our proposed ISC. Block diagrams for (a) traditional sensor system, (b) near-sensor computing, and (c) proposed in-sensor computing.

B. Privacy Preservation

Raw biometric data available at edge devices is vulnerable to user-identifiable information leakage. Although data anonymization techniques [11] remove or modify personally identifiable information to prevent individuals from being identified, these kinds of data processing techniques still could fail if attackers learn more than a minimal amount of information about an individual. Instead of modifying real-time raw data ($\psi_R\left(F,t\right)$) with noise, we propose to send

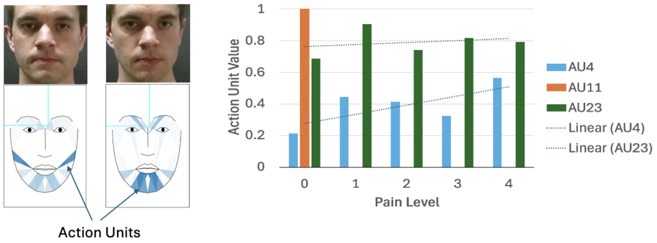


Fig. 3. Pain-level indication leaked by the intensity of muscle contraction detected in action units.

the deviated sensor value ($\Delta\varphi$) from each individual's own baseline ($\psi_B(F,t)$) to the EHR cloud.

$$\Delta\varphi = \psi_B(F,t) - \psi_R(F,t) \quad (1)$$

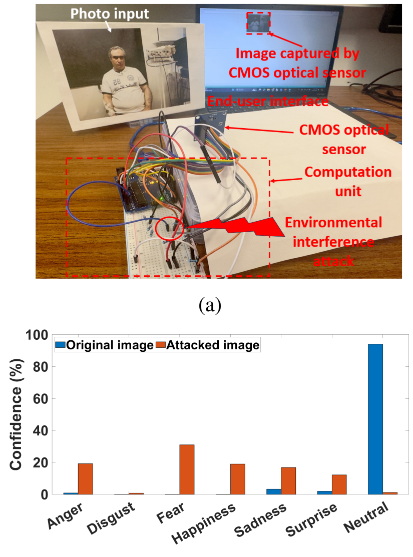
In which, we use *ISC-Config* to implement the desired feature F and only sample the value at moment t. The data pre-processing method is proposed to extract features at edge devices. We adopted a facial expression analysis as a case study. The feature extraction function can be implemented in the ISC computing units to detect the intensity of muscle contraction in Action Units (AUs) [12]. As AUs carry human emotional features, we use machine learning to exploit AU values to differentiate if a person is experiencing pain or not. Figure 3(a) showcases the AUs for a man without and with pain and Fig. 3(b) correlates the pain levels with the AU values. The results confirm that AUs indeed leak pain levels.

C. Security Vulnerability

We examined the new ISC-based edge devices to identify new attack surfaces of an ISC-based system. Given the high integration degree, ISC architecture will be vulnerable to new attacks, including environmental interference attacks and device modeling attacks. We developed a proof-the-concept example to demonstrate a board-level ISC system is vulnerable to a low-cost environmental interference attack. This ISC system captures a facial expression image via a CMOS optical sensor and then utilizes the Py-Feat machine learning model [13] to classify emotions. The experimental setup is shown in Fig. 4(a). Figure 4(b) shows that the environmental interference attack altered the classification result (from neutral to other emotions). This demo indicates that the resilience of ISC systems against harsh environments will be increasingly important than traditional sensor-based computing systems.

III. Conclusions and Future Work

Despite various protection mechanisms available in the cloud for EHR systems, distributed sensor networks at user ends are still vulnerable to cyberattacks, which challenge the security and privacy of EHR. The proposed in-sensor computing architecture provides a new paradigm for cloud-based EHRs to preserve user-identifiable information at sensors. Our preliminary work shows that this paradigm shift is promising to address the increasing threats from cyberattacks. However, the new architecture needs more investigation to ensure its own resilience against security attacks on new surfaces.



(a)

(b)

Fig. 4. Environmental interference attack on an optical-sensor-based ISC for facial-expression-based emotion recognition. (a) Experimental setup for an ISC system for emotion detection and (b) impact of temperature interference on detection accuracy.

Acknowledgment

This work was partially supported by U.S. NSF Independent Research and Development plan and NIH-INBRE Award P20GM103506.

References

[1] "Latest trends in medical monitoring devices and wearable health technology." https://www.businessinsider.in, 2019.

[2] J. Jusak and et al., "A new approach for secure cloud-based electronic health record and its experimental testbed," *IEEE Access*, vol. 10, pp. 1082–1095, 2022.

[3] H. Y. Hossain MM, "Trends and characteristics of protected health information breaches in the united states," in *AMIA Annu Symp Proc. 2020*, pp. 1081–1090, 2020.

[4] N. Farhadighalati, N. Farhady Ghalaty, S. Nikghadam-Hojjati, E. Marchetti, and J. Barata, "Safe-health: A secure framework for advancing edge-based health 5.0," in *2023 WF-IoT*, pp. 1–6, 2023.

[5] M. Tahaei, J. Bernd, and A. Rashid, "Privacy, permissions, and the health app ecosystem: A stack overflow exploration," in *Proceedings of the 2022 European Symposium on Usable Security*, EuroUSEC '22, 2022.

[6] K. Schwab, A. Marcus, J. Oyola, W. Hoffman, and M. Luzi, "Personal data: The emergence of a new asset class," in *An Initiative of the World Economic Forum*, pp. 1–40, 2011.

[7] T. Wan, B. Shao, S. Ma, Y. Zhou, Q. Li, and Y. Chai, "In-sensor computing: Materials, devices, and integration technologies," *Advanced Materials*, vol. 35, no. 37, p. 2203830, 2023.

[8] M. Kajol and Q. Yu, "New security challenges towards in-sensor computing systems," 2025.

[9] A. El Gamal and H. Eltoukhy, "Cmos image sensors," *IEEE Circuits and Devices Magazine*, vol. 21, no. 3, pp. 6–20, 2005.

[10] H. Zhu, Q. Wei, F. Qiao, Y. Yang, X. Liu, x. Shuzheng, and H. Yang, "Cmos image sensor data-readout method for convolutional operations with processing near sensor architecture," pp. 528–531, 10 2018.

[11] K. J. Andrew J, Eunice RJ, "An anonymization-based privacy-preserving data collection protocol for digital health data," *Frontiers in Public Health*, 2023.

[12] F. W. V. . H. J. C. Ekman, P., *Facial action coding system*. Research Nexus eBook, 2002.

[13] J. H. Cheong, E. Jolly, T. Xie, S. Byrne, M. Kenney, and L. Chang, "Py-feat: Python facial expression analysis toolbox," *Affective Science*, vol. 4, 08 2023.

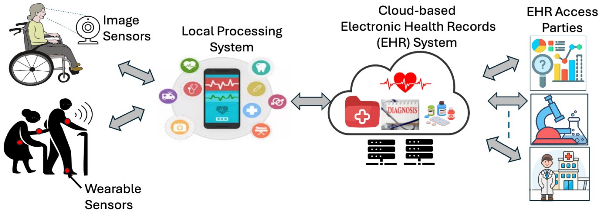
Leveraging In-Sensor Computing to Preserve Privacy in Remote Health Monitoring

Mashrafi Kajol[1], Nishanth Chennagouni[1], Andrew Lu[2], Wei Lu[3], Dean Sullivan[1], and Qiaoyan Yu[1]

[1]University of New Hampshire [2]Oyster River High School [3]Keene State College

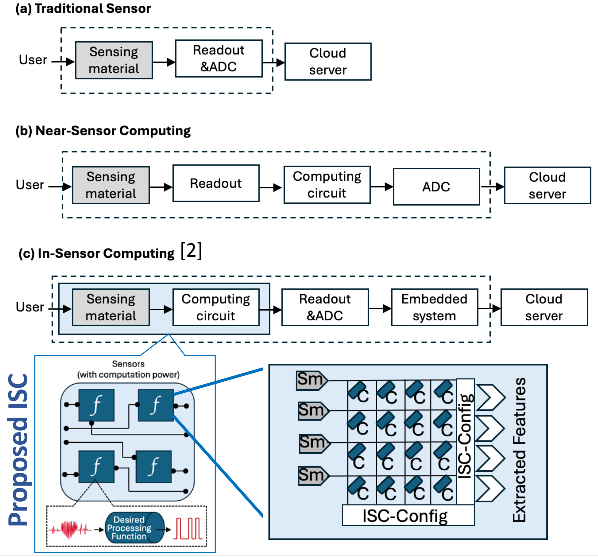
Introduction

- Cloud-based Electronic Health Records (EHR) systems to facilitate remote health-monitoring applications.
- Cyberattacks[1] in EHR harm the benefits of users, diagnosis parties, healthcare providers, and EHR enterprise
- User end devices are not protected yet



Proposed New ISC Architecture

- Different than existing sensor-based computing systems (a) and (b), we introduce a new in-sensor computing system (c) .


(a) Traditional Sensor

(b) Near-Sensor Computing

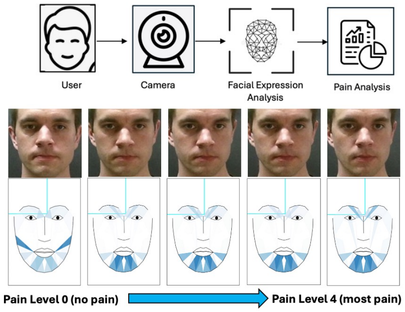
(c) In-Sensor Computing [2]

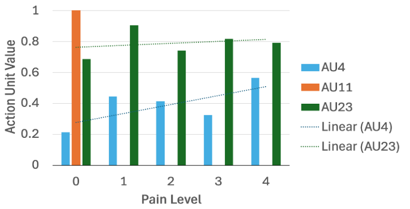
Contribution on Privacy Preservation

- Raw biometric data available at edge devices is vulnerable to user-identifiable information leakage.
- Anonymization techniques still could fail.
- We propose to send the deviated sensor value from each individual's own baseline to the EHR cloud

$$\Delta\varphi = \psi_B\,(F,t) - \psi_R\,(F,t)$$

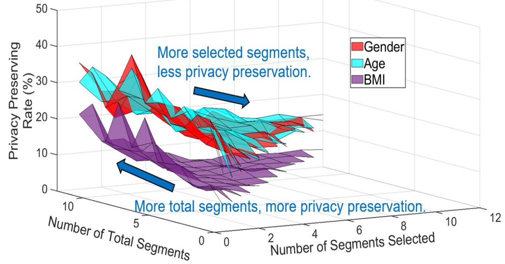
- We propose a data pre-processing method to extract features (AUs[3]) at edge devices





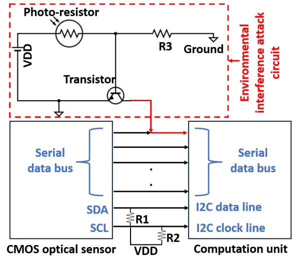
Evaluation of Privacy

- The ML-based Human Activity Recognition (HAR) was performed by a Multi-Task Convolutional Neural Network (MTCNN) with four convolutional layers.
- Feature extraction before machine learning can effectively improve privacy preservation.



Contribution on Security Vulnerability

- We examined the new ISC-based edge devices to identify new attack surfaces of an ISC-based system.
- ISC architecture will be vulnerable to new attacks, including environmental interference attacks and device modeling attacks



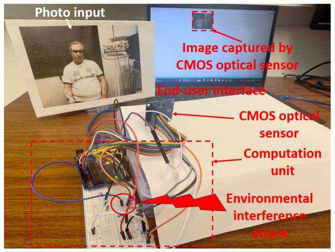
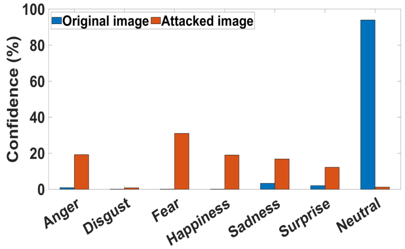


Photo input
Image captured by CMOS optical sensor
End-user interface
CMOS optical sensor
Computation unit
Environmental interference attack



Conclusions

- Distributed sensor networks at user ends are still vulnerable to cyberattacks.
- Proposed in-sensor computing provides a new paradigm to preserve user identifiable information.
- Security attack interfaces need more investigation.

Acknowledgements

- NSF Independent Research and Development plan
- NIH-INBRE award #P20GM103506

References

[1] Hossain et. al., AMIA Annu Symp. Proc. 2020
[2] Wan et. al., Advanced Materials, 35(27), 2023
[3] Ekman et. al., Research Nexus eBook, 2022