THESIS PROJECT PORTFOLIO

E-Skin Resistive Strain Sensor: Optimum Sensor Placement

(Technical Report)

Applying Homomorphic Encryption as a Solution to Privacy Concerns in Artificial Intelligence-Based Medical Diagnostic Algorithms

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Zachary Holden

Spring, 2022

Department of Mechanical Engineering

TABLE OF CONTENTS

Essentially, my science, technology, and society (STS) and technical projects seek to effectively support innovation in the healthcare industry by evaluating the sociotechnical implications of cutting-edge clinical data collection and analysis procedures. Driven primarily by heightened consumer interest in health and wellness tracking from the COVID-19 pandemic, global spending on wearable devices is projected to total $93.9 billion in 2022 (Laricchia, 2022). Interestingly, this widespread public adoption is occurring even though current wearable devices like the Apple Watch, Oura Smart Ring, and Fitbit can only evaluate—with questionable accuracy—a limited range of biophysical signals that have minimal clinical relevance in actuality (Ray et al., 2019). For enhanced precision and efficiency, these devices often rely on artificial intelligence (AI)-based solutions to assist with monitoring and diagnosis; however, this requires access to sensitive health information, which introduces a host of glaring privacy-related concerns. Accordingly, the combined projects serve to answer the overarching research question of "How can we improve clinical diagnostic procedures to improve accuracy and accessibility while properly maintaining user confidentiality?"

The technical project engages the complete lifecycle design of a mechanical skin-like strain sensor from conception to prototype to practical operation. Ultimately, this is aimed at demonstrating the replicability of an existing model that utilizes popular, cost-effective, and commercially available materials and engineering processes. Designed to capture the dynamic motions of the human body with particular applications in clinical diagnostics (i.e., movement and neurological disorders) and athletic performance monitoring, the prototype is intended for placement on the anterior deltoid (shoulder). As such, it features resistive strain sensors in a 4x2 array aligned to optimally measure uniaxial strain along the muscle fibers In terms of composition, the sensor was developed using a thin-film polydimethylsiloxane (PDMS)

elastomeric substrate base with channels of multi-walled carbon nanotube (MWCNT) conductors laminated to its surface. First, a layer of PDMS was poured into a mold, and then channels were etched out of the substrate surface with a laser cutter. Afterwards, MWCNTs were spread into the channels, and a final sealant layer of PDMS was poured overtop. Using gauge factor (GF) as a performance metric, initial testing demonstrated the prototype's ability to consistently generate precise resistance measurements. Additionally, the substrate-skin interface was functional, but future work should attempt to promote steadier conformability by decreasing thickness from 3.5mm.

On the other hand, the STS project explores the viability of using state-of-the-art fully homomorphic encryption (FHE) schemes to develop privacy-preserving machine learning (PPML) models for clinical diagnostics. From a purely technological perspective, FHE, which allows for encrypted data to be processed as if it were unencrypted, seems like a tenable solution, yet further analysis is necessary to analyze the surrounding socio-political effects of deploying FHE-equipped PPML models in the medical industry. Employing the Phase, Guarantee, and Technical Utility (PGU) Triad—a targeted framework for PPML model analysis—as a guide, the ensuing study determined that purely FHE-based solutions do not in fact provide comprehensive privacy protection, considering they are still susceptible to membership inference attacks if the models are constructed via machine learning as a service (MLaaS). Nevertheless, FHE is still a particularly appealing option since it can fortify proven deep neural networks with privacy-preserving functionalities at a negligible accuracy loss. Thus, the results establish that the ideal diagnostic PPML solution would apply FHE in tandem with another approach that obscures the potential information extracted by examining model behavior.

I have found working on both projects simultaneously to be remarkably beneficial in uncovering their deep-rooted associations. In this way, I was able to develop more resolute conclusions that would not have been possible if the two had been performed as completely separate, independent entities. While the work on the technical portion helped me to recognize that the quality of gathered data is a direct product of the quality of the physical instrument taking the measurements, the work on the STS portion provided me with the unique understanding that privacy-based social and political factors can affect the ways in which this data is interpreted. Naturally, this concerted benefit was all the more powerful given the substantial value that was derived from each individual project: the technical project suitably demonstrated the ability to use elastomeric substrates and MWCNTs to improve the conformability—and in turn the usability and accuracy—of wearable devices, while the STS project demonstrated a hybrid PPML approach that can be used to address privacy concerns in existing AI-based medical diagnostic algorithms. Future work should look deeper into how to combine the results of the projects into a complete system that can apply the strain sensor to collect data with a working diagnostic PPML model to interpret the results.

References

Laricchia, F. (2022, Feb. 14). *Global wearable device end-user spending by category 2019-2022*. Statista. https://www.statista.com/statistics/1065271/wearable-devices-worldwide-spending/

Ray, T. R., Choi, J., Bandodkar, A. J., Krishnan, S., Gutruf, P., Ghaffari, R., & Rogers, J. A. (2019). Bio-integrated wearable systems: A comprehensive review. *Chemical Reviews*, *119*(8). 5461-5533. https://pubs.acs.org/doi/10.1021/acs.chemrev.8b00573