# Biometric Identification in Healthcare

* I was thinking about researching how people are trying to implement biometric ID into healthcare.
  + The below are AP citations, plan to change to IEEE but google scholar does not list that as an option.
* 1 Mason, J., Dave, R., Chatterjee, P., Graham-Allen, I., Esterline, A., & Roy, K. (2020). An investigation of biometric authentication in the healthcare environment. *Array*, *8*, 100042.
  + <https://www.sciencedirect.com/science/article/pii/S2590005620300278>
  + Intro
    - Begins with definition of Biometrics: “is the measurement of a human being using the physical and behavioral characteristics.”
    - Brings up Jane Doe in hospital, and how biometric technologies could help identify them. Even how smartphones are using similar technology to easy peoples use.
    - This article, will explore the periocular region and how if it is suitable for phones then it should be similarly suitable for health care.
    - Then will move to collecting the data from patients
    - Then they will go into acceptance rates and modes and modules of use.
  + Biometric Systems
    - Factors for identifiable biometrics: everyone has,
    - “Uniqueness means that the characteristic should be sufficiently differ to distinguish”
    - “permanence implies that the characteristic is not varying over time.”
    - “measurable […] should be able to measure easily”
    - “accuracy of the system based on operational requirements”
    - “acceptability indicates the comfort of individual”
    - “circumvention relates to the ease[…] of using fraud”
    - Periocular: almost unchanged with age, irises are unique (as discussed in class), many sets of data can be formed in the region which leads to higher accuracy.
  + Biometric system functionality
    - System modes: enrollment and verification
    - Enrollment: data is captured, “… stored in a template within the database.”
    - Verification: reference model created, samples are matched, testing process conducted
    - “a one-to-many evaluation is performed with the biometric templates from the database to establish the identity”
    - Mechanisms to Biometric system:
    - Sensor “where the biometric information of the user is captured.”
    - Feature extractor: “processed to extract feature values”
    - Matching conducted
    - Decision making
    - System Performace:
    - “depends on the hardware configurations, the software used, the tools selected, ..”
    - External factors have high impact on ability to identify.
  + Healthcare systems
    - Possible problems of access and expenses.
    - Explanation of current healthcare system
    - MPI (master patient index) reduces redundancies and links record across providers.
  + Related Works
    - Discussion on wrong patient problems
    - Multifactor authentication proposed
  + Proposed Periocular Module
    - Deep learning method
    - Keeping a super database to hold the info of all patients from the different MPI’s discussed earlier
    - In their tests, using an iphone 5 and galaxy s4 were able to collect and identify individuals with accuracy of 90.31 after 20 iterations.
  + Conclusion
    - Add this on as a multi factor authentication to help identify patients and start building the records in the databases.
* 2 Banville, M. C. (2023). AM I WHO I SAY I AM? THE ILLUSION OF CHOICE: BIOMETRIC IDENTIFICATION IN HEALTHCARE.
  + <https://thescholarship.ecu.edu/bitstream/handle/10342/12822/BANVILLE-DOCTORALDISSERTATION-2023.pdf?sequence=1&isAllowed=y>
  + 37, 92
  + This study more focused on the ability to connect surveillance and biometrics and how historically excluded different groups
  + Biometrics was designed as a surveillance tool
  + “nurses in the study discussed how facial recognition technologies used on them in healthcare setting, but not necessarily used in day-to-day”
  + Discussed how fingerprinting was more popular
  + “creates a sense of illusion that because the technology is assisting the healthcare facility, if patients do not comply “
  + This compliance could make it difficult to collect data or test identity
  + This book also brought the points up I was wondering in the last article, “What data is collected, where is it stored, third party access”
* 3 Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., & Gide, E. (2021). A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services. *Sensors*, *21*(2), 552.
  + <https://www.mdpi.com/1424-8220/21/2/552>
  + Intro
    - “access for dispersed clinical information” from IBM and Aetna sounded super shady and they are throwing that n the first paragraph.
    - This article was discussing could computing and IOT for healthcare as storage and access which could solve some of the issue brought up in other articles
  + Background and Why
    - Already used in areas like “fitness programs, age care applications, and remote health”
    - “Biometric information is considered confidential by nature.” Helping to limit “the risk of information leakage.”
    - Also required to be encrypted
  + System challenges
    - Again brings in a large collected database that different providers, users all have access to as “its inherent cross-domain access”
    - “do not disclose identifiable information to the provider without the user’s consent” (many points of failure in terms of security.)
  + Limitations
    - “tested to be secure against spoofing attacks.”
    - “man in the middle and replay attacks are yet to be tested”
  + Conclusion
* 4 Buhagiar, E., & De Raffaele, C. (2021). An Effective Biometric Patient Identification System for Health Organizations.
  + <https://personales.upv.es/thinkmind/dl/journals/lifsci/lifsci_v13_n12_2021/lifsci_v13_n12_2021_9.pdf>
    - Intro
      * “2.6 million people die each year […] due to medical errors, including errors of patient identification.”
      * “The main three reasons include incorrect patient identification at the point of registration, time pressure when treating patients, and thirdly, lack of employee training and awareness.”
    - Wrist bands
      * Wristbands with barcodes to scan are the main method of Id currently
      * Improved errors by 12-57%
    - Privacy
      * “patients refused to be subject to such technology due to privacy and confidentiality concerns.”
      * “safeguards must be set down for every step, from collection to retention of the data collected.”
    - Security
      * Security flaws
        + DoS, Intrusion, Repudiation, Function creep
    - Limitations
      * Discussed different issues arising due to lighting, masks, injury, age.
    - Results
      * Concerns “included security, accuracy, cost, and patient cooperation.”
* 5 Singh, G., Bhardwaj, G., Singh, S. V., & Garg, V. (2021). Biometric identification system: security and privacy concern. *Artificial intelligence for a sustainable industry 4.0*, 245-264.
  + <https://link.springer.com/chapter/10.1007/978-3-030-77070-9_15>
  + Intro
    - Opened with another definition of biometrics and a discussion of their uniqueness to each human.
    - Discused and reestablished the trait by mason (universality, uniqueness, accuracy, reliability and acceptability.
  + Biometric modalities
    - Finger prints, facial scans, hand measurements , palm scans, iris scans, vocals
  + Issues in Biometric system
    - Biometric encryption is weak
    - Current problems with time to access the data as well.
    - Author proposes that the “power of the computer is enhancing day by day, this will help in finding the solution in very less time and calculations”
    - “few foreign particles like dust and moisture on the scanner surface can wrongly present the data.”
  + Advantages and Disadvantages
    - “increasing its importance around the globe.”
    - “people believe and trust more on modern biometric systems in comparison to traditional security systems.”
    - “complex system”, “non tech-friendly can be flopping in the pool of technical people to understand the system.”
* 6 Ahamed, F., Farid, F., Suleiman, B., Jan, Z., Wahsheh, L. A., & Shahrestani, S. (2022). An intelligent multimodal biometric authentication model for personalised healthcare services. *Future Internet*, *14*(8), 222.
  + <https://www.mdpi.com/1999-5903/14/8/222>
  + Intro
    - This article is discussing personalized healthcare devices that consistently collect data on patients to attempt to provide key insights to their health and help make recommendations.
    - To help make sure it is the right patient, this article proposed the use of biometrics to identify the patients.
    - Like Buhagiar, the thought to use “a few common biometric traits such as ECG and PPG” and deep learning.
    - In specific for this article, they are discussing medical device safety
  + Security Analysis
    - Impersonation and spoofing attacks
      * “IoT attacks are prone to spoofing attacks”
      * Only checking in the beginning of a session, these devices if taken in the middle could lead to an attacker getting the users data
    - Injection and tampering attacks
      * “networks that adopt the proposed authentication approach is also secure from an injection attack”
      * Using biometrics at the network level would leave attackers unable to penetrate these networks
    - Registration phase attack
      * “imposter can register a rough device into the network during registration.”
      * This is attempted to be mitigated through two step registration and multifactor authentication.
  + Discussion
    - In their experiment they had 100% authentication and 99.92% accuracy using ECG only
  + Limitations
    - “User authentication has room for further improvement”
    - “we did not explore DDoS, side-channel attacks, or man in the middle attacks”
* 7 Mwapasa, M., Gooding, K., Kumwenda, M., Nliwasa, M., Kaswaswa, K., Sambakunsi, R., ... & Desmond, N. (2020). “Are we getting the biometric bioethics right?”–the use of biometrics within the healthcare system in Malawi. *Global Bioethics*, *31*(1), 67-80.
  + <https://www.tandfonline.com/doi/full/10.1080/11287462.2020.1773063>
  + Intro
    - First mention on DNA analysis as a way to biometricly ID someone
    - Brings back to the view of healthcare
    - “potential advantages, such as reducing medical errors, reducing the risk of fraud and improving capacity to react to medical emergencies”
    - Ethical issues:
      * Data security
      * “ensuring that peronal health records are appropriately protected from unauthorized use and patient confidentiality s maintained”
  + Results
    - “confusion amongst some patients […] about why they were supposed to have their fingerprints scanned.”
    - Why did they think that was only for the illiterate?
    - Discussion of limited knowledge of the area of biometrics from patients and staff.
    - “other factors associated with power imbalance in client-provider relationships which led to a lack of questioning on the part of the client”
    - Fear from patients about their confidentiality from experiences with Malawian healthcare passports that stated HIV status giving providers stigmas against them.
    - Happy to strengthen access to healthcare records
    - Restriction to richer or higher population areas once again
  + Discussion
    - “biometric identification would be welcomed and considered ethically appropriate, if undertaken in a manner that ensured that the benefits of implementation for patients outweighed potential harms.”
    - Brings back the point of user and patient training and education.
* 8 Dargan, S., & Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Systems with Applications*, *143*, 113114.
  + <https://www.sciencedirect.com/science/article/pii/S0957417419308310>
  + Intro
    - “To achieve robustness, high accuracy rates and difficult to spoof are the main factors that generally distinguish from the traditional methods for the security.”
    - Discusses different methods of measuring biometrics. “holistic class and feature class”
    - Advantages
      * Security
      * Convenience
      * Reliable identifiers
    - Disadvantages
      * Sensitivity
      * Identity leakage
      * Current sample sizes
      * Privacy risks
  + Need for Biometrics
    - Discusses flaws with password or token based systems
    - “Biometric systems are not the replacement of authentication and security tools and technologies but combining biometric approaches with these tools can increase the security aspects.
  + Analysis and discussion
    - Improvements in the technologies over the years
    - More sure of a persons identity
    - Worry about data safety
    - Multi model and multi factor authentication