ADVANCECRT

Centre for Research Training

Science Foundation Ireland sfi For what's next

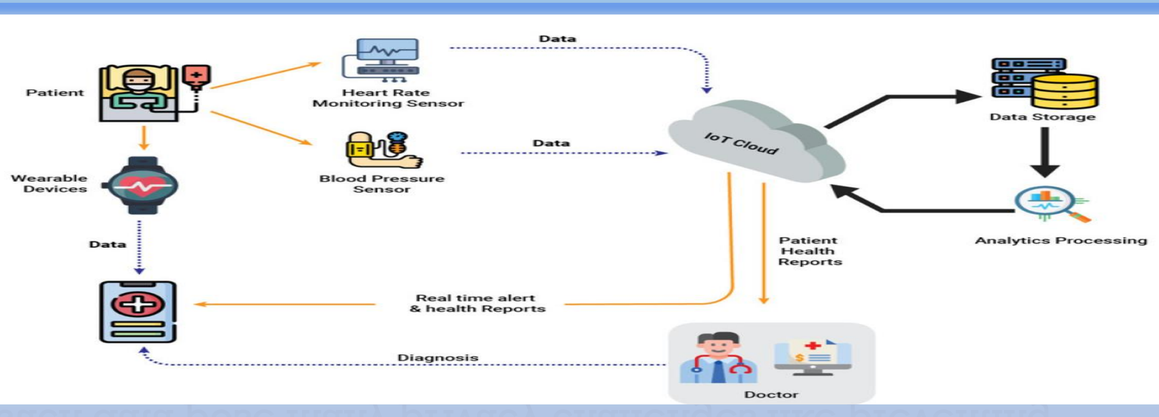
Privacy in the Medical Internet of Things

Ramin Soleimani

Supervisors: Prof. Dirk Pesch and Prof . Donna O'Shea

Introduction

- The Medical Internet of Things is exponentially growing, This technology is playing a more and more important role in public health and safety.
- Thanks to IoT technology, patients can be monitored continuously. They don't need any more to see their medical caregivers in many cases.
- A huge amount of medical data produced by IoT devices raises serious concerns regarding the privacy preservation of the patients during different stages of the data life cycle.
- On one hand, the collected data
- offer remarkable opportunities for data-driven analytics, personalized recommendations, and actionable insights.[1] On the other hand, the processing, utilization, and distribution of such data pose many privacy challenges like preventing individual identification, sensitive information disclosure, targeted profiling, and mass identity theft.[2]
- Privacy is "the claim of individuals, groups, or institutions to decide for themselves when, how and to what extent information about them is communicated to others" [3].
- The data life cycle has several stages: collecting, transmission, storage, and use phases.



https://embeddedcomputing.com/

What are we going to address in this research?

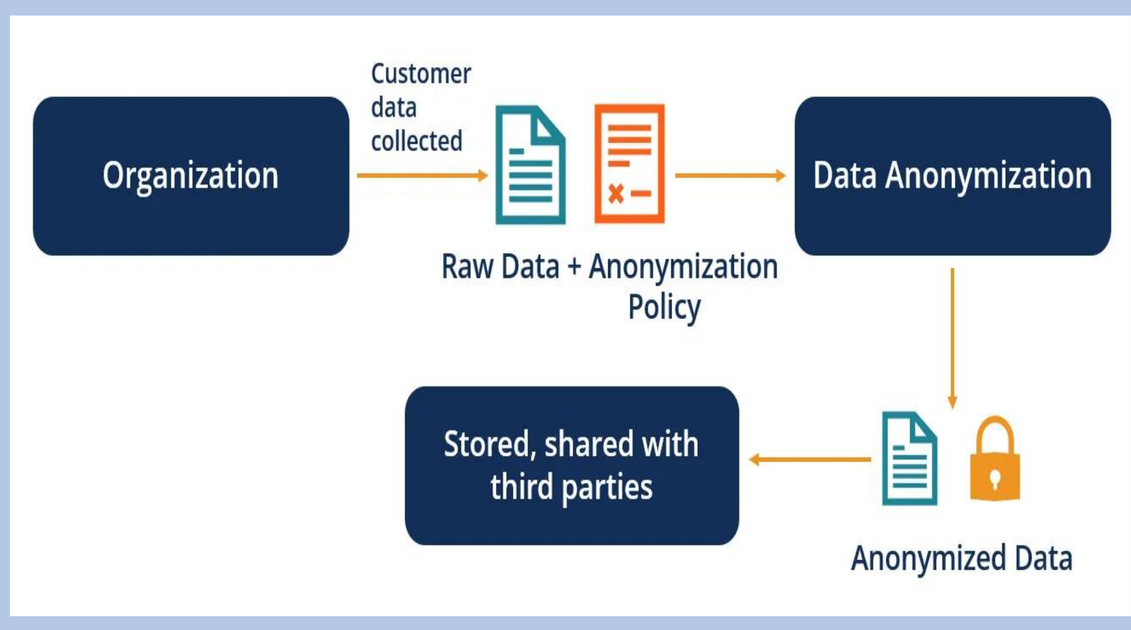
- This research aims to provide proper solutions that address privacy preservation issues surrounding medical data in IoT applications.

Challenges

- limited resources available in IoT devices have left medical data vulnerable to malicious attacks that can breach data privacy.
- Recently, due to advances in machine learning (ML) tools, privacy protection has become more challenging.

Solutions

- Existing privacy techniques can be categorized into two groups: data perturbation and data restriction
- Data perturbation: these techniques are a series of operations that modify or hide some sensitive parts of the original data to preserve privacy [2]. Noise addition and anonymization are two methods in this category.
- Data Restriction Techniques: these techniques are focused on restricting data use by blocking access or encrypting data. Data restriction techniques include access control and crypto-based methods.



https://www.techfunnel.com/

Industrial contributions

- In the medical industry, since patient information is so sensitive to disclose, the privacy preservation of medical data is becoming a challenging issue of the medical IoT. Thus privacy preservation is highly required to ensure a reliable medical IoT network.

References

1. Wieringa, P. Kannan, X. Ma, T. Reutterer, H. Risselada, and B. Skiera, "Data analytics in a privacy-concerned world," J. Bus. Res., vol. 122, pp. 915–925, 2021
2. K. M. Chong, "Privacy-preserving healthcare informatics: A review," in Proc. ITM Web Conf., 2021, vol. 36, Art. no. 04005
3. Westin, A.F.: Privacy and freedom. Wash. Lee Law Rev. 25(1), 166 (1968)
4. Fang, W., Wen, X.Z., Zheng, Y., Zhou, M.: A survey of big data security and privacy preserving. IETE Tech. Rev. 34, 1–17 (2016)

Host Institution

University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

MTU Ollscoil Teicneolaíochta na Mumhan Munster Technological University

Maynooth University National University of Ireland Maynooth

Ollscoil Teicneolaíochta Bhaile Átha Cliath Dublin Technological University Dublin

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin