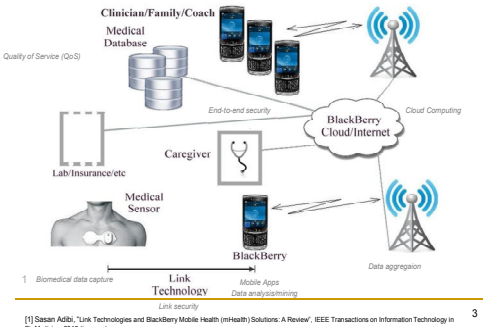
RMIT UNIVERSITY

Privacy Enabled Mobile-Health (mHealth)-based Diabetic Solution

Sasan Adibi, Ph.D.
Senior IEEE Member, Research Fellow
Business IT & Logistics Department, RMIT University, Melbourne, VIC, Australia
May 14-16, 2012

Contents

The mHealth's Big Picture



[1] Sasan Adibi, "Link Technologies and BlackBerry Mobile Health (mHealth) Solutions: A Review", IEEE Transactions on Information Technology in BioMedicine, 2012 (in press)

Continuous Glucose Monitor (CGM) and Insulin Pump (IP)

CGM is an invasive tool (needle-based) that is used in a patch-shaped device, attached to the patient's body and continuously monitors the glucose level in the blood stream[2].

Insulin is a hormone that causes cells in the muscles, liver, and fat tissues to take up glucose from the blood and store it as glycogen in the liver and muscles[3].

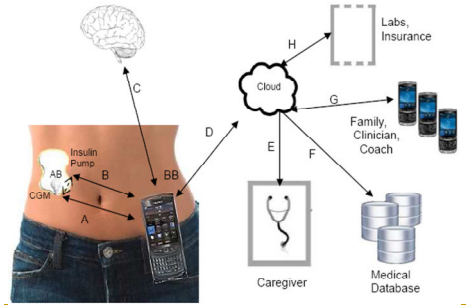
Biomedical Applications – Bitrates

1

Biomedical Application	Maximum Data Rate (kbps)
Blood Pressure	10
Heart Pulse Rate	10
Respiration	10
Glucose Monitoring	**10**
Thermometer	10
Blood Oxygen – Pulse Oximeter (SpO2)	1
Weighing Scale	1
Electrocardiography (ECG/EKG) - 12 leads	300
ECG (6 leads)	100
Electromyography (EMG)	300
Electroencephalogram (EEG) - 12 leads	50
Motion Detection	50
Cochlea Implant	100
Artificial Retina	700
Still Image	2000
Video	1000
Audio	1000
Voice	100

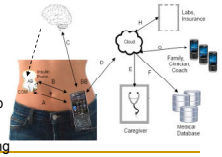
[1] Sasan Adibi, "Link Technologies and BlackBerry Mobile Health (mHealth) Solutions: A Review", IEEE Transactions on Information Technology in BioMedicine, 2012 (in press)

Artificial Pancreas Platform



Artificial Pancreas Platform, *Cont'd*

- Interactions between the Smartphone and CGM **(A)**
- Interactions between the Smartphone and IP **(B)**
- Interactions between the IP and CGM **(AB)**
- Interactions between the user/Smartphone **(C)**
- Interactions between the user/IP/CGM **(--)**
- Interactions between the Smartphone/Cloud **(D)**
  - Cloud ←→ user
  - Cloud ←→ IP
  - Cloud ←→ CGM
- Communication and Security Protocols
- Security
  - Privacy, integrity, anonymity, DoS, Non-Rep
- Quality of Service, benchmarking
  - Scalability, interoperability, Cloud-Computing



Privacy Requirements

- **Network Perspective[4]:**
  - End-to-end Privacy
    - Authentication and Indentity management/concealment (privacy)
      - Suite-B featuring Elliptic Curve Cryptography (ECC)
        - Biometric Authentication and Authorization
    - User-based Data integrity and privacy
      - Hashing and encryption, biometric-based
      - Adaptation to the user-data-history and acess protection
    - Non-repudiation
      - Biometric-based digital signature

Privacy Requirements, *Cont'd*

- **Privacy-by-Design Requirements[5]:**
  - Proactive-not reactive, preventative not remedial
  - Privacy as the default setting
  - Privacy embedded into design
  - Full functionality – positive-sum, not zero-sum
  - End-to-end security – full lifecycle protection
  - Visibility and transparency
  - User-centric privacy

References

1. **Sasan Adibi, "Link Technologies and BlackBerry Mobile Health (mHealth) Solutions: A Review", TITB-00277-2011, 10.1109/TITB.2012. 2191295, IEEE Transactions on Information Technology in Biomedicine**
2. **Hemoglobin, Wikipedia, http://en.wikipedia.org/wiki/Glycated_hemoglobin**
3. **Insulin, Wikipedia, http://en.wikipedia.org/wiki/Insulin**
4. **Sasan Adibi, "An application layer non-repudiation wireless system: A cross-layer approach", PhD thesis, Electrical and Computer Engineering Dept., University of Waterloo, September 27, 2010**
5. **Ann Cavoukian, "Privacy-By-Design Principles", adapted from http://privacybydesign.ca, May 09, 2012**