Arizona State University

AzTE Arizona Technology Enterprises

www.azte.com

Physiology Based End-to-End Security For Life-Long EHR Management

AzTE Case # M13-244P

Inventors

Dr. Sandeep Gupta

Associate Professor

School of Computing, Informatics, and Decision Systems Engineering

Dr. Ayan Banerjee

Postdoctoral Research Assistant

School of Computing Informatics and Decision Systems Engineering

Background

In mobile healthcare (mHealth) systems, a network of wireless monitoring sensors and actuators worn by a patient communicate with the cloud through a base station (usually a smartphone) to monitor and administer medical treatment. A patient's electronic health records (EHRs) are stored in the cloud and are routinely updated with new data. Ensuring the security of data is crucial, not only for patient confidentiality, but also safety as a data breach could result in erroneous diagnosis and treatment. Current methods only secure the transmission of data through user-defined password protection, which can be especially cumbersome when a patient has multiple EHRs. Additionally, username-password security requires that data pass through a smartphone, leaving the patient vulnerable to greater risk should the smartphone be compromised.

Invention Description

Researchers at ASU have developed protocol that provides a secure communication channel by encrypting a patient's medical data using their unique electrocardiogram (ECG) and photoplethysmogram (PPG) signals. EHRs can be securely created, managed, combined, or updated without redundant manual authentication, and cannot be accessed without the patient's most recent ECG and PPG signals. The protocol can be used with a smartphone, or a sensor with Wi-Fi or mobile capabilities that communicates directly with the cloud. The protocol does not involve heavy processing which is ideal for battery powered sensors, and has no pre-deployment or security requirements. Once a secure channel has been established, the model's parameters are continuously updated with the patient's physiological information and rekeying is automatic. Should there be a significant change in a patient's ECG or PPG signals (e.g. after heart surgery), the new physiological information can be updated through a doctor's authorized account.

Intellectual Property Status:

Pending

Potential Applications

- EHR Management
- End-To-End Security
- Machine-To-Machine Communication
- Physiology Based Encryption

Benefits and Advantages

- **Automatic** – Once a secure channel has initially been established, no user intervention is needed to manage EHRs or update security configurations.
- **Efficient** – Does not involve heavy computer processing, saving battery life in remote sensors.
- **Increased Security**
  - End-to-end physiology based encryption requires current patient data to hack
  - Allows for direct communication between sensors and the cloud.
- **Longevity –** Can potentially last the entire lifetime of a patient.
- **Versatility**
  - Can be combined with other end-to-end security techniques.
  - Can be used with or without a base-station or smartphone.

Contact

Bill Loux

Director of Business Development, Physical Sciences

Arizona Technology Enterprises, LLC (AzTE)

P: 480.884.1992

F: 480.884.1984

BLOUX@AZTE.COM

TECHNOLOGYVENTURES@AZTE.COM