# Investigation of the Internet of Things in its Application to Low-cost Authentication within Healthcare

Fatemeh Tehranipoor, *Student Member, IEEE*, Nima Karimian, *Student Member, IEEE*, Paul A. Wortman, *Student Member, IEEE*, and John A. Chandy, *Senior Member, IEEE*

***Abstract*— In this paper we propose a low-cost solution to design concerns for the application of IoT devices for authentication within healthcare domain based on the use of physical unclonable functions (PUFs) and biometrics.**

## I. Introduction

There are benefits provided by IoT technologies to the healthcare domain and the resulting applications can be grouped mostly into: tracking of objects and people (staff and patients), identification and authentication of people, automatic data collection and sensing [1]. Unfortunately, IoT is extremely vulnerable to attacks for several reasons. First, physical attacks to the unattended components are easy. Second, since most of the communications are wireless, eavesdropping is extremely simple. Third, IoT components cannot implement complex schemes to support security since they are characterized by limited resources and capabilities. Therefore, an authentication framework for IoT in e-Health is a necessary requirement in any information system to ensure the availability of information to authorized users only.

## II. Proposed Security Approach for Authentication

Risks of applying IoT in healthcare include possible harm to the patient's safety and health, loss of protected health information and unauthorized access to devices and exploits of vulnerabilities. Therefore, one must address the limitations and security concerns of the underlying hardware (*IoT device*) and authentication process (*patient authorization*) to be sure that both patients and staff are equally protected from malicious, or erroneous, behavior.

### A. Device Verification

Counterfeit hardware is a problem that plagues embedded systems and IoT medical devices. PUFs are one of the solutions commonly used to authenticate electronic devices. PUFs generate unique IDs by exploiting the uncontrollable process variations associated with modern integrated circuit fabrication. An ideal PUF takes an input (challenge) and gives a random output (response) which is unique for every device; Ideally, there should be an exponential number of possible challenge-response pairs.

### B. Patient Authentication

While monitoring patients remotely, collecting data and protecting them from tampering, it is very crucial to reduce the impact level of the risk factor to address security and privacy concerns. We propose using bio-signals for patient authentication because of their potential uniqueness, universality, and resistance to spoofing. Electrocardiogram (ECG) signals are such a bio-signal that can be used not only for the purpose of diagnosis and treatment, but also can be used for biometric authentication and key generation [3].

F. Tehranipoor, N. Karimian, P. A. Wortman, and J. A. Chandy are with the Electrical and Computer Engineering Department at the University of Connecticut, Storrs, CT 06269 USA (corresponding author to provide e-mail: fatemeh.tehranipoor@ uconn.edu).

### C. Proposed Solution

An overview of our security approach is illustrated by Figure 1. This approach is split up between a device *verification step* and a *patient authentication* step. During the device verification step, the healthcare IoT device's trust is established. A PUF challenge-response pair can be used to validate the trustworthiness of IoT operation. Ideally, the PUF should be low-cost such as a DRAM-based PUF [2] which uses existing memory on the IoT device. Should this verification fail, then the device cannot be trusted and thus will not be used for reading biological signals. If authenticated, the IoT device can then be used to read the biological signals and perform the necessary processing to produce a 'bio-key' [4]. This 'bio-key' is then enrolled in a health care provider database allowing for later authentication of a given patient to the medical staff. This step, of course, requires encryption techniques.

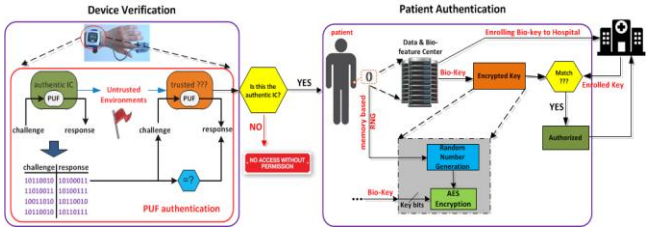


Figure 1. Security Approach for Low-Cost Verification of Devices and Patients.

## III. Conclusion

Through our solution, presented in this paper, one can establish that the information produced from an IoT is trustworthy, that the individuals accessing information can be properly identified, and that the exchange of sensitive biological signals across a network is secure.

## References

[1] A. Vilamovska et al., "Rfid application in healthcare–scoping and identifying areas for rfid deployment in healthcare delivery," RAND Europe, February, 2009.

[2] F. Tehranipoor et al., "DRAM-Based Intrinsic Physically Unclonable Functions for System-Level Security and Authentication." *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* (2016).

[3] N. Karimian et al., "Highly Reliable Key Generation from Electrocardiogram (ECG)." *IEEE Transactions on Biomedical Engineering* (2016).

[4] N. Karimian et al., "Evolving authentication design considerations for the Internet of biometric things (IoBT)." *Hardware/Software Codesign and System Synthesis (CODES+ ISSS), 2016 International Conference on*. IEEE, 2016.