# Chapter 13
# Securing the Human Cloud: Applying Biometrics to Wearable Technology

**Pallavi Meharia**
*University of Cincinnati, USA*

**Dharma Prakash Agarwal**
*University of Cincinnati, USA*

## ABSTRACT

*Wearable technology is rapidly changing the way we associate objects with our surroundings, and how we interact with the objects. As technology becomes more commonplace in our surroundings, our lives are rendered more vulnerable. As technology becomes more sophisticated, our interaction with it seems to become progressively minimalistic. This chapter introduces techniques wherein secure communication between humans and their surrounding devices can be facilitated by applying human physiological information as the identifying factor. Different biometric techniques are investigated, and the rationale behind their applicability is argued. Additionally, the benefits and possible use-cases for each technique is presented, and the associated open research problems are brought to light.*

## INTRODUCTION

For most, the Internet of Things (IoT) is largely a buzzword associated with a diffused layer of sensors, actuators and devices aimed at collecting data with the goal of forwarding the same to the Internet. The underlying technological goals and applications which enterprise the need for IoT will truly revolutionize the way we perceive our world and our own interaction with it. IoT is geared towards greater machine to machine communication; built on cloud computing services and sensor centric data-collection networks. With an aim of providing real-time, virtual and mobile connection, it will render technology to be truly ubiquitous and "smart". By integrating a wide range of varied technologies into a synergetic framework, pervasive computing will provide enhanced tools of greater economic amalgamation. An analysis of the IoT infrastructure brings to light the fact that humans form a very complex network, and possibly

DOI: 10.4018/978-1-5225-5484-4.ch013

the lowest strata of the architecture upon which the IoT is based on. If we analyze the framework for wearables and IoT, they can be classified into the following connected networks (Figure 1): (a) Smart Body: Body area network, (b) Smart Life: Personal area network (house, car, work, etc.), and (c) Smart World: Wireless sensor networks (street, buildings, infrastructures).

At the other end of the spectrum, with the guaranteed omnipresence of such technology comes the stagnating truth of 24x7 surveillance or what is commonly known as the "Big Brother" syndrome. With the idea of adopting embedded devices into everyday devices gaining rapid interest, the need to design and develop security solutions aimed at satisfying the unique constraints of IoT devices is higher than ever. The three major challenges which question the feasibility of the IoT architecture have been identified as: (a) ubiquitous data collection, (b) exploitation of consumer data, and (c) unprecedented security risks (Swan, 2012). A key concern to bear in mind with this unique technology is that it is as much as a software problem as a hardware one.

Caught in this crossroad, many researchers have suggested the use of biometric based solutions towards fortifying the IoT infrastructure, thereby paving the way for an Identity of Things security suite. Biometrics is defined as the automated recognition of an individual based on their physiological or behavioral characteristics. While the term biometrics does invoke the thought of security driven products into the mind, it does not automatically correlate to wearable technology at the first instant. However, there has been a rise in the demand of biometric based security solutions, to facilitate secure communication in wearable devices. The feasibility and relative ease of implementation make them a suitable candidate for devising a security suite designed to serve the needs of an IoT infrastructure. While not new in concept, biometric characteristics have been proposed and widely applied for physical authentication purposes.

*Figure 1. The Internet of Things forms a heterogeneous network architecture consisting of: (a) Wireless Body Area Networks (b) Wireless Local Area Network (c) Wireless Metropolitan Area Network and (d) Wireless Area Network*