Chapter 4
Confidential Data Storage Systems for Wearable Platforms

Mingzhong Wang
University of the Sunshine Coast, Australia

Don Kerr
University of the Sunshine Coast, Australia

ABSTRACT

With the features of mobility, reality augmentation, and context sensitivity, wearable devices are widely deployed into various domains. However, the sensitivity of collected data makes security and privacy protection one of the first priority in the advancement of wearable technologies. This chapter provides a study on encryption-based confidentiality protection for data storage systems in wearable platforms. The chapter first conducts a review to storage solutions in consumer wearable products and explores a two-tier, local flash memory and remote cloud storage, storage system in wearable platforms. Then encryption-based confidentiality protection and implementation methods for both flash memory and remote cloud storage are summarized. According to the interaction and integration of these two components, a categorization of confidential storage systems in wearable platforms is proposed. In addition, the benefits and selection criteria for each category are also discussed.

DOI: 10.4018/978-1-5225-1016-1.ch004

INTRODUCTION

With the ever-increasing computational power along with decreasing cost, microprocessor chips in tiny sizes are becoming wearable. That is, they can be embedded into clothes, personal accessories, and even bodies (Mann, 1997). With the development of wearable technologies, a new computing paradigm is emerging. In comparison with traditional computers, which are machines separated from their users, wearable devices are attached to our bodies, extending the limitation of our bodies with various capabilities of sensing, communicating, and computing (Roggen, Magnenat, Waibel, & Troster, 2011).

With the features of mobility, reality augmentation, and context sensitivity, wearable devices can be applied in various domains, including military and medical monitoring and emergency response (Billinghurst & Starner, 1999). In recent years, the popularity of wristbands, smart watches, and the buzz around Google Glass signaled the success and wide acceptance of wearable technologies.

Although wearable devices come in various sizes, shapes, and capacities, they are generally designed to perform data collecting and processing tasks. In essence, they are a tiny version of connected computers. Since wearable devices are directly attached to human bodies, the data gathered, such as health measurements and GPS locations, are usually highly linked to users' privacy. For example, activity trackers and smart watches can measure users' heart rates, precise steps, sleeping quality, and sometimes locations. The leakage of these data enables unauthorized parties to assess and predict the lifestyle and health conditions of the users. Insurance companies may use these data to increase health premiums, or even to cancel a policy. The risk and fear of exposure of these sensitive data is one of the major inhibitors to the adoption of wearable technologies (Al Ameen, Liu, & Kwak, 2012).

The flow of data in wearable technologies involves the stages of data sensing, local processing, local storage, and transmission to remote server or storage. Security or privacy breaches generally occur in the storage and transmission stages. However, traditional security and privacy preserving solutions cannot be applied directly to all categories of wearable devices with varied hardware capacity, including processors, RAM, power supply, and communication rage (di Pietro & Mancini, 2003). Especially, due to the size and weight constraints, the battery capacity in wearable devices becomes a major restriction from providing rich functionality (Huang, Badam, Chandra, & Nightingale, 2015).

Solutions for secure communications between wearable devices and storage server have been widely studied (Al Ameen et al., 2012; di Pietro & Mancini, 2003; Starner, 2001). However, limited literature can be found for the research on secure and confidential storage management in wearable platforms. Therefore, this chapter