Chapter 50
Analyzing the Security Susceptibilities of Biometrics Integrated with Cloud Computing

John R. Regola
Pennsylvania State University – Altoona, USA

Brandon R. Baez
Pennsylvania State University – Altoona, USA

John K. Mitchell III
Pennsylvania State University – Altoona, USA

Syed S. Rizvi
Pennsylvania State University – Altoona, USA

ABSTRACT

In the present scenario, the vulnerabilities associated with cloud computing and biometric technology rank among the most vital issues in information security. In this chapter, the primary goal is to investigate the physical and informational security susceptibilities of biometrics, analyze the structure and design possibilities of the cloud, and examine the new developments of biometrics with cloud computing. Foremost, the authors analyze the developments of biometrics and compare the performance based on defining characteristics. In addition, they examine threats and attacks that can compromise the assets of an organization or an individual's sensitive information. Furthermore, this chapter provides a comprehensive discussion on the physical vulnerabilities of biometrics. Moreover, one section of this chapter focuses on the informational and database vulnerabilities. In this chapter, the authors also discuss the design considerations and cloud computing paradigm in relation to biometric security systems.

INTRODUCTION

The development of biometric technology has improved exponentially within the last few decades (Sabena, Dehghantanha, & Seddon, 2010). The ever-evolving advancements in this field address security issues that, for many years, security professionals have been trying to remedy. There are two basic classifications of biometrics: physiological and behavioral. In the case of physiological, scanners measure size, shape, and uniqueness of physical characteristics of the human body (More, Ubale, & Jondhale,

DOI: 10.4018/978-1-5225-0983-7.ch050

2008). The verification of an individual's identity using physiological biometrics is solely reliant on input that cannot be altered by the users. For instance, fingerprint scanners identify the variations between the ridges, loops, and whirls within a fingerprint, which is unique to every individual. An iris scanner identifies the intricate structures within an iris, patterns that no two humans share. In contrast, behavioral biometrics is the classification that involves monitoring the consistency of behavior in an individual's input, including, but not limited to, gait, voice recognition, and palm pressure scanning.

The results in these identification entries are subject to variation, and as a result often face issues such as FAR and FRR. FAR refers to the instances in which the scanner falsely grants access to a biometric system. On the contrary, the FRR refers to instances in which the scanner falsely rejects access to a biometric system. Since lowering the FAR would increase the FRR, they need to be balanced in what is known as the equal error rate (EER) (Kukula, Sutton, & Elliott, 2010). The EER is the rate of equality between the FAR and FRR (Kukula, Sutton, & Elliott, 2010).

In order to reduce the FAR and FRR, while maintaining a high level of accuracy, multimodal biometrics can be applied. There are two major types of multimodal systems: intra-class and inter-class. This refers to the use of either multiple layers of the same technology or integrating multiple forms of biometric systems (Chin Ong, Goh, & Hiew, 2009). For example, a multimodal security system can comprise of either different types of fingerprint scanners (such as optical and thermal scanners) or a fingerprint scan followed by an iris scan. Later, in the development of biometric technology section, we will provide several examples of how multimodal biometrics can be implemented.

Currently, there are at least three main characteristics shared among many of the common biometric security systems that we previously discussed. The robustness, intrusiveness, and distinctiveness are qualities that relate to identifying an individual (Govinda & Ngabirano, 2012). Robustness refers to a trait that is subject to change over a period of time. Meanwhile, intrusiveness revolves around the comfort of the individual and their personal privacy when using the biometric system. A less intrusive biometric security system is ideal for acceptance by society. Distinctiveness relates to the variations in a specific trait contained by the general population. The greater the level of distinctiveness, the more exclusive the system would be. These characteristics enable us to compare and contrast them in an effort to understand the advantages and disadvantages of different biometric security systems.

Fingerprint scanning, is fairly robust and highly distinctive, especially when compared to dynamic signature verification. However, there is still a chance that some individuals have unusable fingerprints due to aging or an injury. In general, a conclusion can be made that pattern or geometric scanning is more robust than dynamic scanning. This is evident by the low level of robustness seen in dynamic signature verification and keystroke dynamics (Govinda & Ngabirano, 2012). Another factor to consider is the level of intrusiveness, since fingerprints only require a touch rather than a retinal or facial scan. These require static positioning and keen observation.

In terms of retinal scanning and iris recognition, they are highly robust and distinctive, making it very efficient in terms of accuracy and performance. The iris and retina are less likely to change over time when compared to fingerprints or voice recognition. Similarly, the patterns of a fingerprint and both the iris and retina are randomly formed giving uniqueness to their respective traits. This allows for a very high level of distinction since there are no two patterns alike.

To obtain optimum biometric performance, the scalability issues need to be addressed. The cloud is the best solution for such a matter of contention. The structure of the cloud allows for shared network resources that contain the memory, CPU, and storage. There is less hardware and software required by the user since it becomes the responsibility of the service provider. One of the features of cloud computing