**Case Project 11-4: Standard Biometric Analysis:**

* Even the biometrics can be defined as the reliable and effective way for authentication, it, also has disadvantages, such as:

1. Costs

The costs of biometric software, devices and servers are higher than other types of authentication tools. In a 2018 survey by Spiceworks, 67 percent of IT professionals cite cost as” the biggest reason for not adopting biometric authentication.” Transitioning to a biometrics authentication wouldn’t be the only thing a company would have to pay for, with 47% of the surveyed stating a need to upgrade current systems in order to support a shift to biometric authentication on their devices[1].

### Error Rate:

Biometric devices can make two common types of errors, False Acceptance Rate (FAR), when the device accepts an unauthorized person and False Rejection Rate (FRR), when it rejects an authorized person. The error rate could create big mess for the entire security system. It could happen due to weather, physical condition, age and other issues. A great chaos could happen with an error rate of as low as 1% in a large-scale authentication process.

Standard biometric techniques have different features, advantages and disadvantages. Cost is an important feature to consider when choosing the biometric method.

* Fingerprints is the most popular biometric method. It is the patterns of ridges and valleys on the surfaces of fingers. Fingerprint scanners use sensors to get an image of the finger and determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned image.

The common types of sensors of fingerprint scanners:

1. Optical sensor is the most common when choosing of fingerprint sensors due to its cheap price. Optical sensors pose shortcomings like quality of scan is impacted with dirty fingers and they are easier to be tricked than other types of sensors.
2. Capacitive scanner is more expensive because it is hard to forge and cannot be fooled with fingerprint images.
3. Ultrasonic scanner uses very high frequency sound wave to read pattern of fingerprints. It is not affected by dirtiness of finger surface.
4. Thermal line sensor uses the measuring temperature variation to read a fingerprint pattern of ridges and valleys. It is small-sized and highly costing.

* As much as using of fingerprint scanners is rising and the technology itself is progressing, hackers are working to improve their techniques to break through these scanners in some ways, such as:

## 1. Using Masterprints

Hackers can use masterprints to break into devices with less-powerful scanner that are found in some mobile phones. The high percentage of False Acceptance Rate (FAR) is a big chance of an unapproved fingerprint to access to a system.

## 2. Harvesting Unsecured Images

Hackers can hold the key and get into the scanner when they get a hold of the fingerprint image. Hackers target unattended devices or scanners to get the expected raw fingerprint data. Once the hacker gains access to stored data, he can get the picture and harvest the fingerprint details.

## 3. Using Forged Fingerprints

There are many ways hackers can use to turn the harvested fingerprint to a physical recreation. They can use a wax or wooden replica of a hand or print it on a special paper and use it on the scanner.

## 4. Exploiting Software Vulnerabilities

Using password managers is a handy and effective way to secure passwords but only when the software of the password manager is secured. If the software is not secured enough, hackers can exploit it to get all the details of the fingerprint scan. Purchasing well-known and popular products is the best way to avoid exploiting these vulnerabilities.

## 5. Reusing Residual Fingerprints

Another type of attacks, to use the left over from a previous fingerprint scan on objects to gain access to it. It is exactly like forgetting the key in the door. Avoiding this attack is simply to wipe fingerprint scanners after using.

* All biometric authentication techniques depend on statistical algorithms and are not reliable to use alone. These methods are exposed to have false rejection or false acceptance.

Personally, my recommendation is to use fingerprint technique. It is a common and accurate standard biometric technique that, also, comes very handy to use. But, above all, when compared with other biometric techniques, it does not cost too much.

Sources:

1. More Organizations Are Adopting Biometrics for Security—But Barriers Still Remain:  <https://businessinsights.bitdefender.com/more-organizations-are-adopting-biometrics-for-security-but-barriers-still-remain>.
2. Advantages and disadvantages of biometrics <https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics>.
3. 10 Advantages and Disadvantages of Biometrics System You Should Know: <https://biometrictoday.com/10-advantages-disadvantages-biometrics-technology/>
4. [Biometric Devices: Cost, Types and Comparative Analysis](https://www.bayometric.com/biometric-devices-cost/): <https://www.bayometric.com/biometric-devices-cost/>
5. 5 Ways Hackers Bypass Fingerprint Scanners: <https://www.makeuseof.com/tag/ways-hackers-bypass-fingerprint-scanner/>
6. Biometrics: definition, trends, use cases, laws and latest news: <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics>