BIOMETRIC AUTHENTICATION

FINGERPRINT RECOGNITION

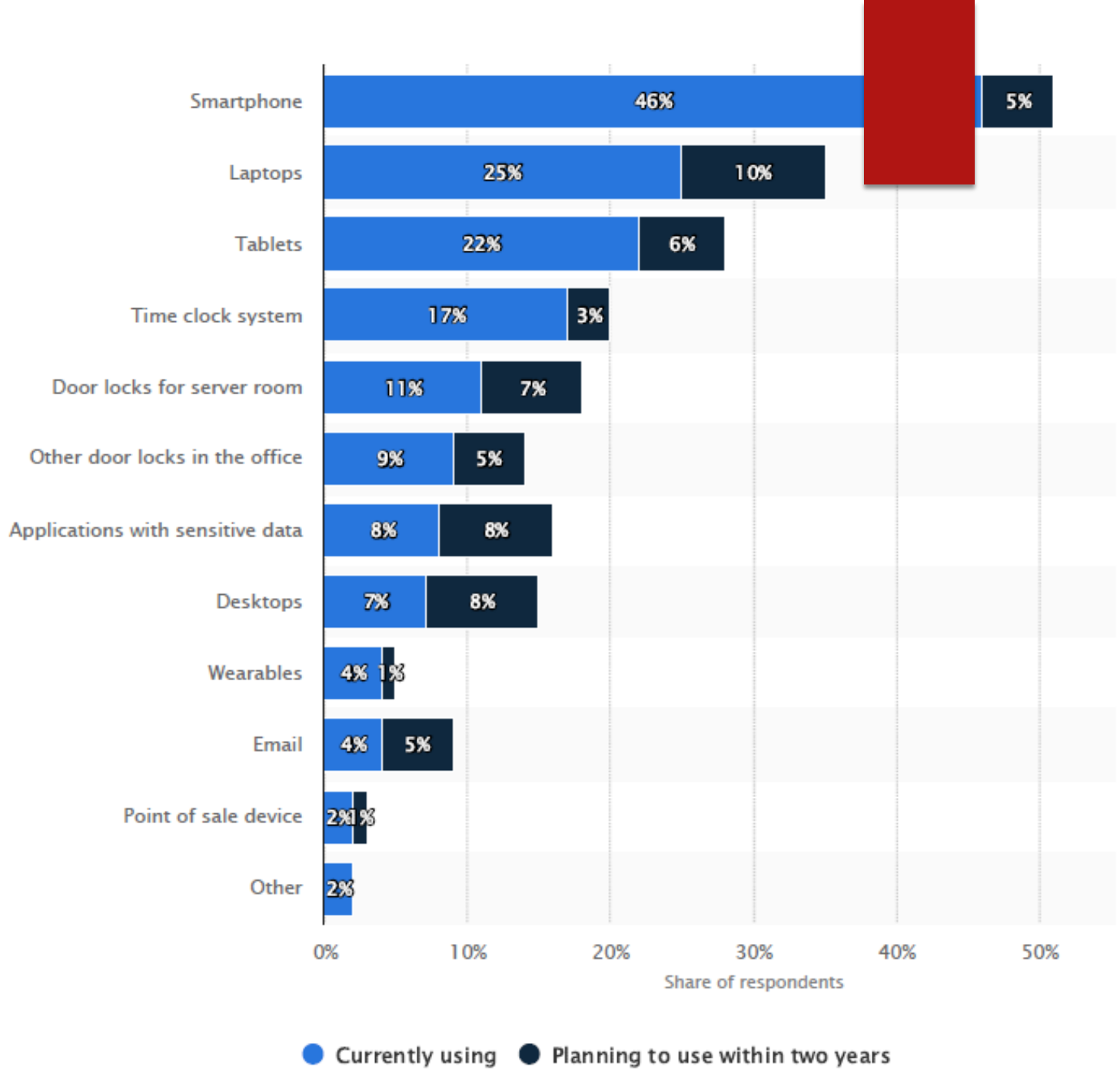
SIDHARTH KALIAPPAN

Outline

- What is Biometric authentication ?
- Why fingerprint?
- Characteristics and features of Fingerprint
- Feature extraction and Matching
- Security and attacks on fingerprint systems
- Spoof detection and prevention
- Personal work

BIOMETRICS

Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he is who he says he is.



https://www.statista.com/statistics/937365/north-america-europe-business-use-biometric-authentication/

BIOMETRICS

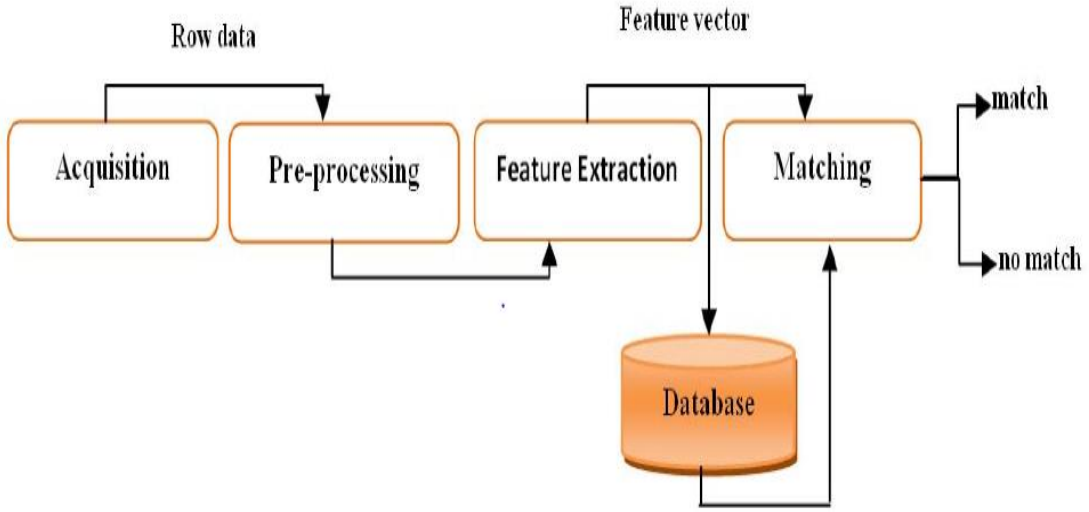
POSITIVES

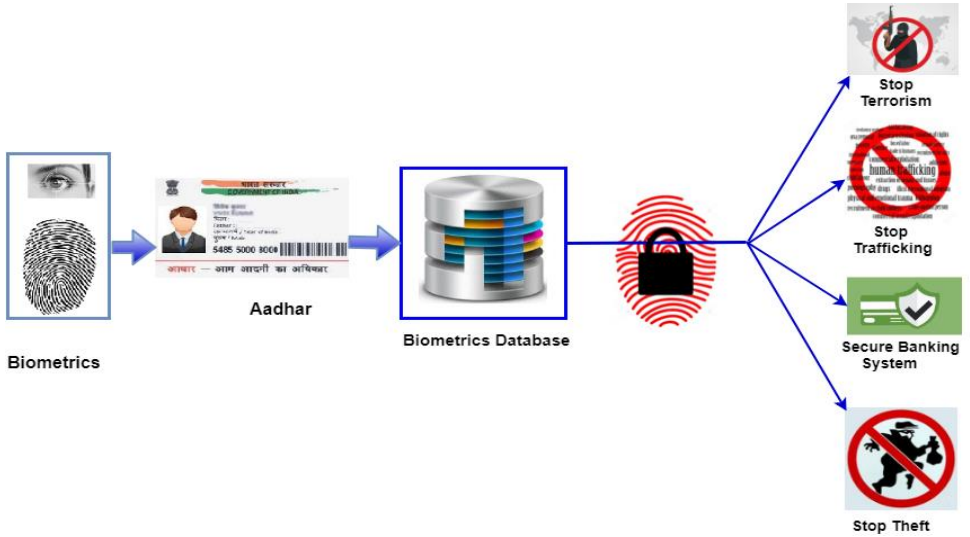
- Convenience
- Security

NEGATIVES

- Remote access
- Lasts a lifetime
- Software issues

BIOMETRIC AUTHENTICATION





https://www.researchgate.net/publication/310953762_Overview_of_Fingerprint_Recognition_System

FINGERPRINT

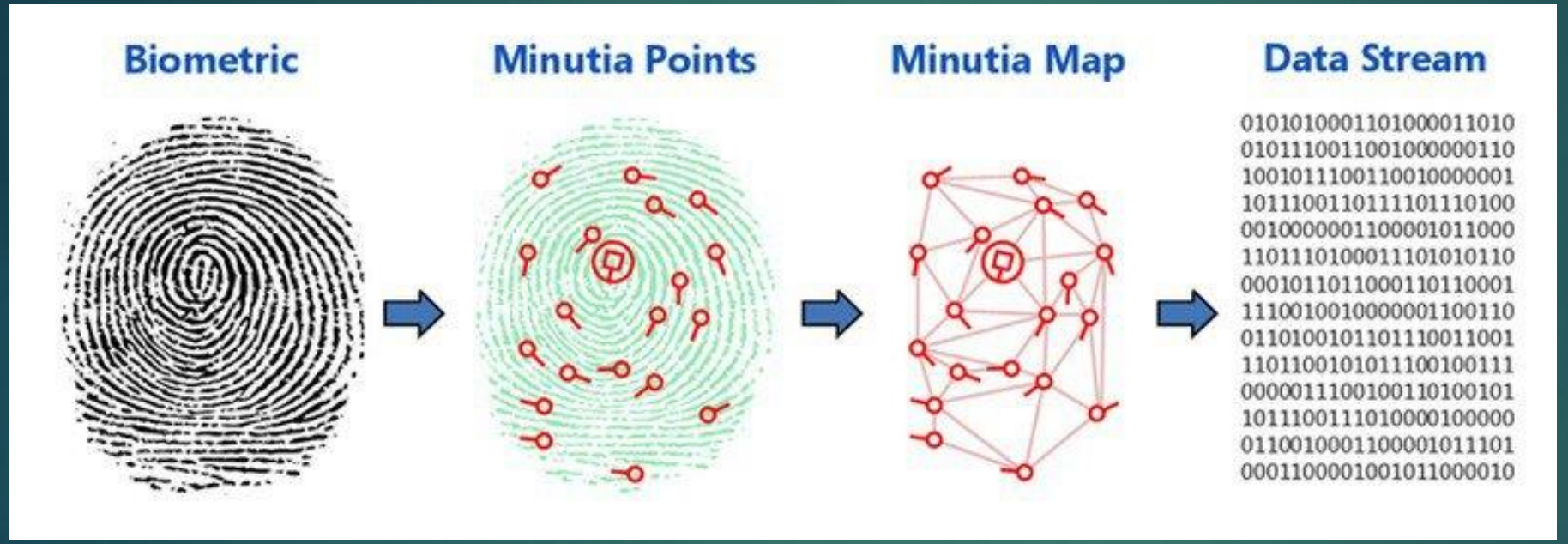
Figure 4 Patterns of fingerprint

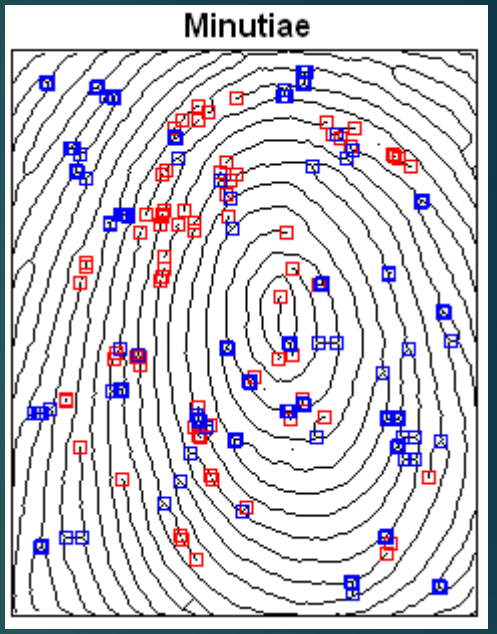
https://www.123rf.com/photo_85214864_stock-vector-three-fingerprint-types-on-white-background-loop-whorl-arch-patterns.html

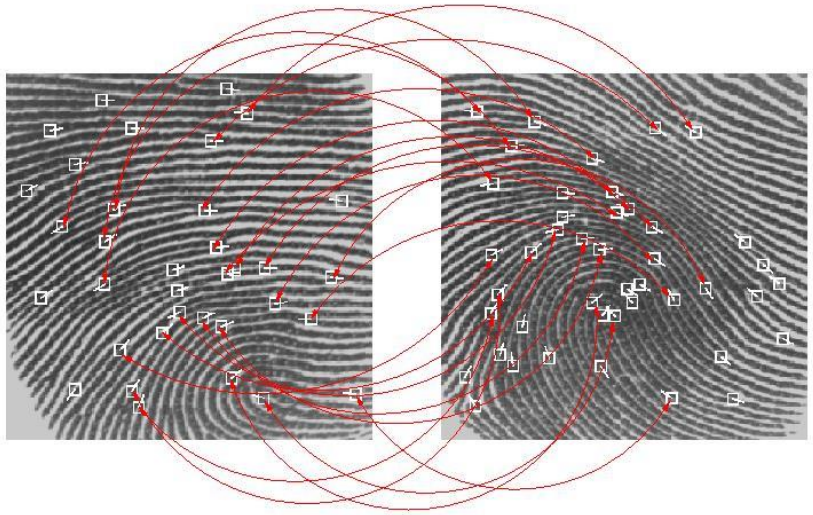
CHARACTERISTICS OF A FINGERPRINT

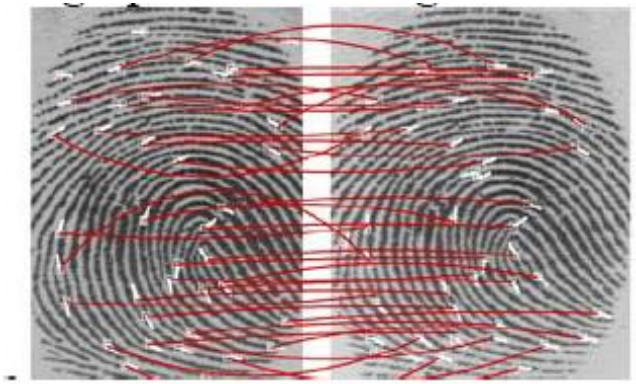
- Ridge dots
- Bifurcations
- Trifurcations
- Ending Ridge
- Ridge crossing
- Islands
- Hooks
- Bridges

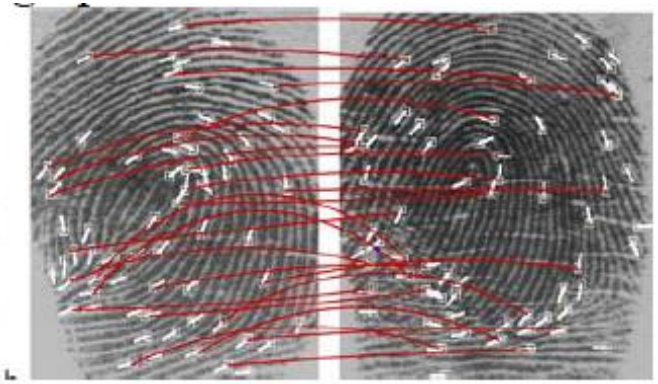
Feature Extraction



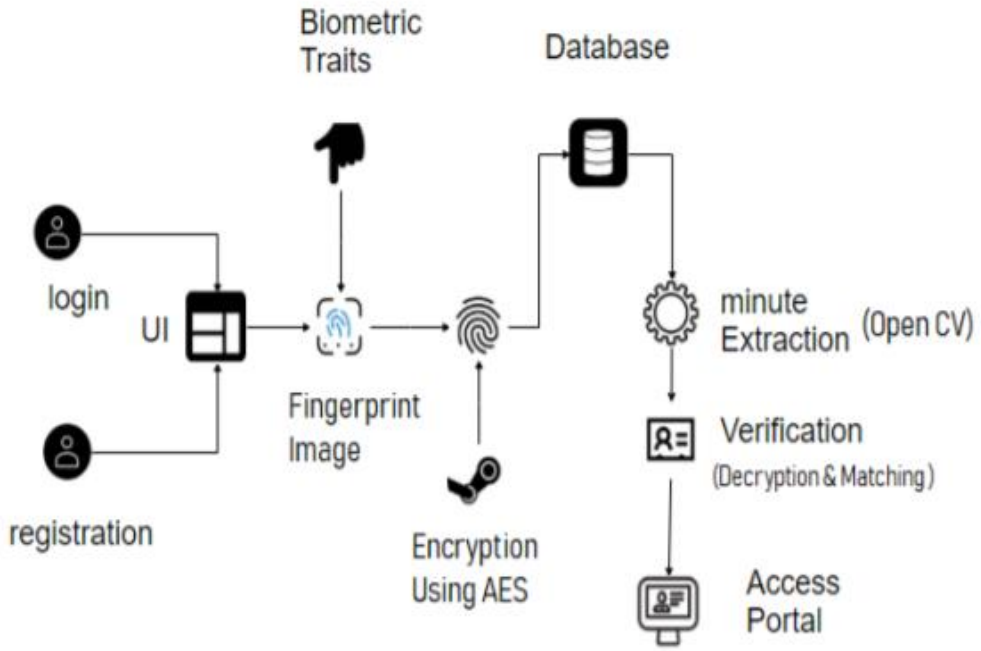




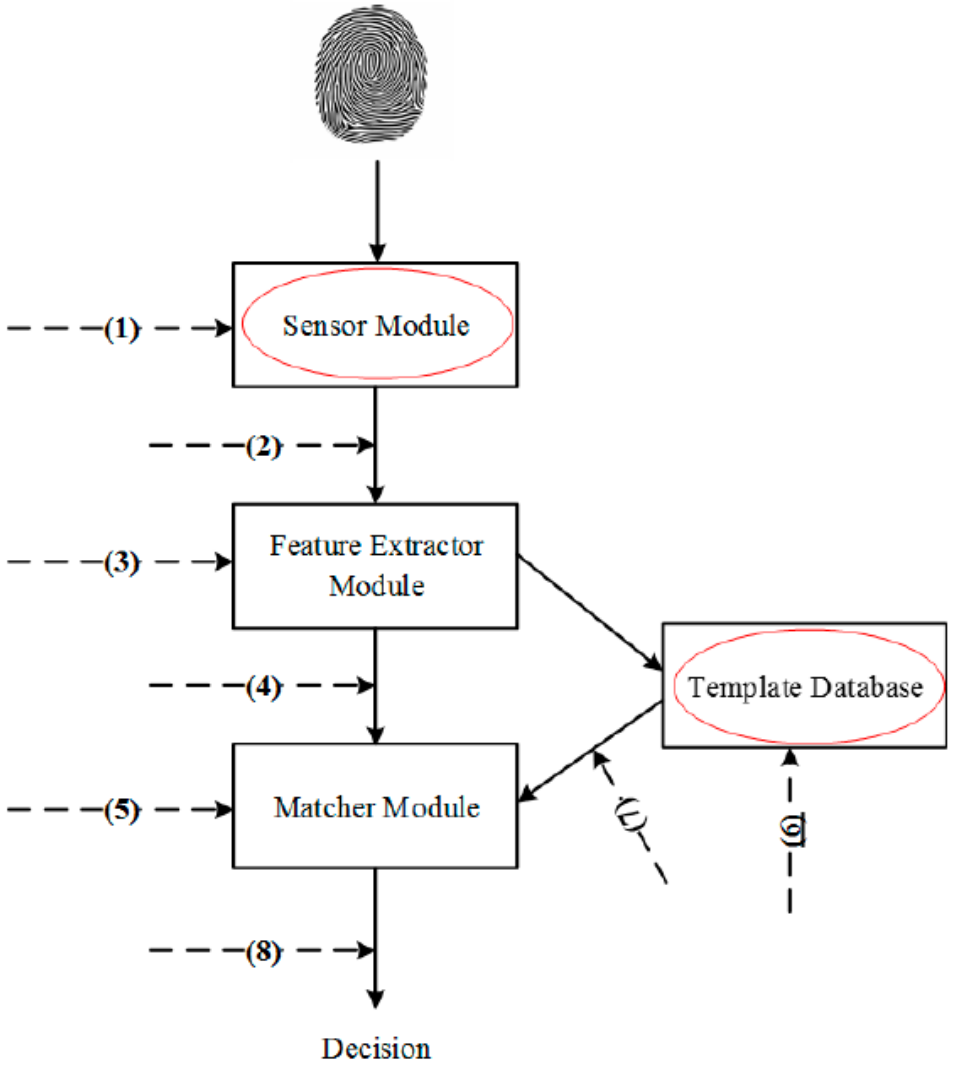




MATCHING


Biometric
Traits
Database
login
UI
Fingerprint
Image
minute
Extraction
(Open CV)
Verification
(Decryption & Matching)
registration
Encryption
Using AES
Access
Portal

Encryption



Attacks and Security

Number	Attacks	Attack Points
1	Spoofing—present fake biometric data to sensor	1
2	Exploit similarity, e.g., using face from identical twins	1
3	Zero-effort attempt—attacker uses own biometric sample to impersonate an authorized user	1
4	Physically destroy the biometric sensor so as to make it out of service	1
5	Replay attack—the attacker intercepts a biometric signal and replay it into the system	2 and 4
6	Cut the communication channel to make the system unavailable	2 and 4
7	Denial of Service attack—alters the information from the channel in order to deny a genuine user from being authenticated	2 and 4
8	Hill-climbing attack—conveniently modify the query image until a desired matching score is obtained.	2 and 4
9	Continuously inject samples in order to deny genuine users to access the system	2 and 4
10	Inject Trojan horse programs	3 and 5
11	Attacker illegally obtains original biometric templates	6
12	Attacker modifies the template such as adding or replacing info	6
13	Read biometric templates from a communication channel and replay	7
14	Alter the information transmitted through a communication channel in order to deny genuine users to access the system	7
15	Cut the communication channel in order to make the system unavailable	7
16	Alter the transported matching or non-matching information in order to deny access of a genuine user or allow an impostor access.	8
17	Cut the communication channel in order to make the system unavailable	8

Types of Attacks

Personal Work

- Biometric software are proprietary.
- The Components are expensive.
- Develop an Open source complete software.
- Compatible with various types of sensors.
- Can be easily integrated with different cloud services.
- Reduce the total cost. (50-60 CHF)

References

- Wencheng Yang 1,* , Song Wang 2 , Jiankun Hu 3, Guanglou Zheng 1 and Craig Valli 1 . Security and Accuracy of Fingerprint-Based Biometrics.
- Yijun Yang, Jianping Yu, Peng Zhang, and ShulanWang, A Fingerprint Encryption Scheme Based on Irreversible Function and Secure Authentication.
- Brinzel Rodrigues 1, Rushikesh Pawar2, Pranay Patil3, Ankit Gour4, Encryption and Decryption of Biometric Traits.
- Arakala, A.; Jeffers, J.; Horadam, K. Fuzzy extractors for minutiae-based fingerprint authentication. In Proceedings of the 2007 International Conference on Advances in Biometrics, Seoul, Korea, 27–29 August 2007; pp. 760–769.
- C. Cattani and G. Pierro, “On the fractal geometry of DNA by the binary image analysis,” Bulletin ofMathematical Biology, vol.75, no. 9, pp. 1544–1570, 2013.