PIP2001 Capstone Project
Review-0

ENCRYPTION OF BIOMETRIC TRAITS TO AVOID PRIVACY ATTACKS

Batch Number: CCS-G24

Roll Number	Student Name
20211CCS0148	Nisha.S
20211CCS0144	Prasthuthi Raj
20211CCS0107	Shreya B
20211CCS0113	Sanika MS
20211CCS0111	Bhoomika BK

Under the Supervision of,

Ms. Raesa Razeen
Professor / Associate Professor / Assistant Professor
School of Computer Science and Engineering
Presidency University

Name of the Program: CSE
Name of the HoD: Dr. Blessed Prince P/Dr. Robin Rohit/Dr.Asif Mohammed H.B
Name of the Program Project Coordinator: Mr. Amarnath J.L & Dr. Jayanthi. K.
Name of the School Project Coordinators: Dr. Sampath A K / Dr. Abdul Khadar A / Mr. Md Ziaur Rahman

Content

- Problem Statement
- Github Link
- Analysis of Problem Statement
- Timeline of the Project
- References

Problem Statement Number:

Organization: AICTE

Category (Hardware / Software / Both) : Software

Problem Description:

Encryption of multimodal features enhances the security for physical characters of biometrics. Bio-crypto system provides the authentication as well as the confidentiality of the data. This project proposes to improve the security of multimodal systems by AES encryption algorithm, generating the biometric key from iris and face biometrics with its feature extraction using machine learning techniques. The secret value is encrypted with biometric key using symmetric Advanced Encryption Standard (AES) Algorithm which is efficient in terms of software implementation and works well on the image data.

Difficulty Level : Meduim

Github Link

The Github link provided should have public access permission.

Github Link

https://github.com/Nisha6471/CCS-G24-CAPSTONE-PROJECT-.git

Analysis of Problem Statement

Technology Stack Components:

* Encryption Algorithms

- **Symmetric Encryption:**

  Algorithms like AES (Advanced Encryption Standard) for encrypting biometric data with a single key.

  Symmetric encryption is fast and suitable for handling large volumes of data.

- **Asymmetric Encryption:**

  Algorithms like RSA (Rivest-Shamir-Adleman) for encrypting encryption keys or smaller amounts of data.

  Asymmetric encryption uses a pair of keys (public and private) and is used for secure key exchange.

- **Homomorphic Encryption:**

  Specialized encryption techniques that allow computations to be performed on encrypted data without needing to decrypt it first.

  This can be useful for biometric matching processes.

- **Secure Hashing:**

  Hash functions like SHA-256 for creating unique, irreversible representations of biometric traits to enhance security.

Analysis of Problem Statement

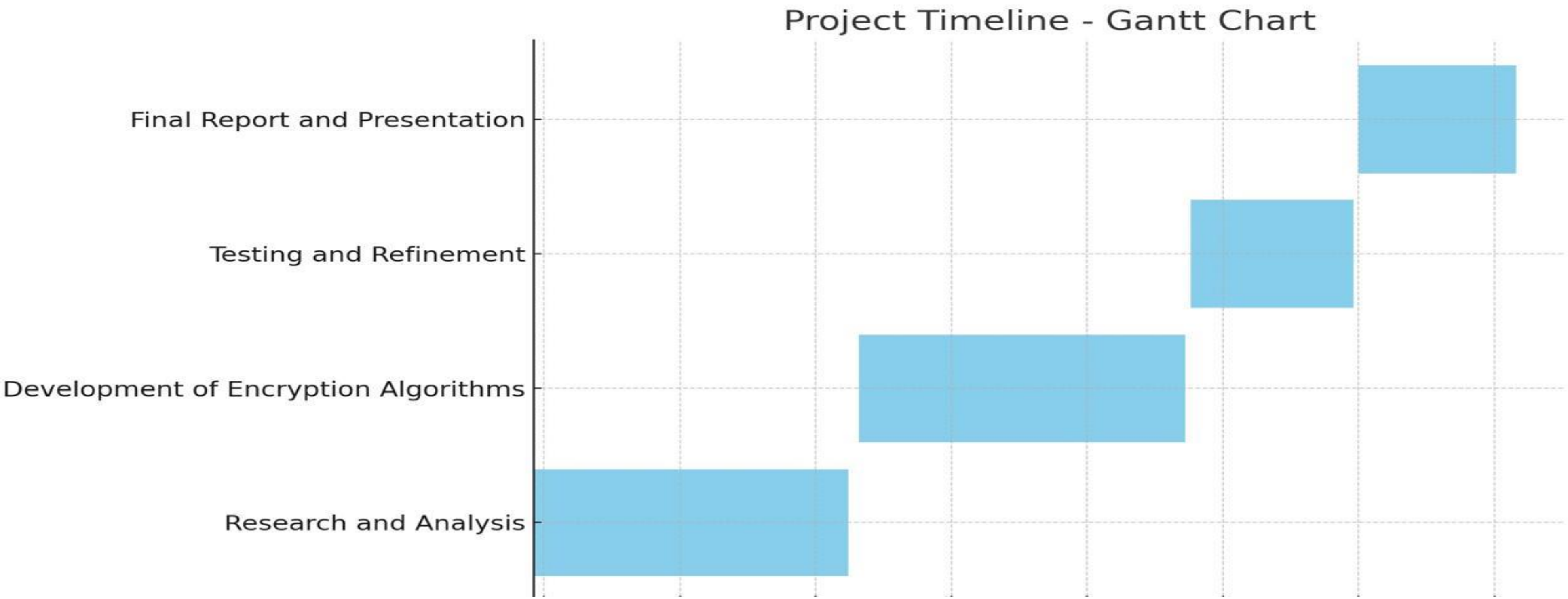
- Biometric Data Processing
- Secure Storage and Access control Management
- Authentication and verification
- Compliance and regulatory Frameworks
- Data Sensitivity and Irreversibility
- Storage and Transmission
- Performance Overhead
- Feature Preservation

Analysis of Problem Statement (contd...)

Software and Hardware Requirements:

- VS Code,
- HTML
- CSS,
- MySQL,
- Python ,
- Webcam.

Timeline of the Project (Gantt Chart)



Timeline of the Project (Gantt Chart)

Research and Analysis: September 2024 -October 2024

Development of Encryption Algorithms: October 2024 - November 2024

Testing and Refinement: November 2024

Final Report and Presentation: December 2024

(it will take around 3 to 4 months)

References (IEEE Paper format)

[1]J. Galbally, S. Marcel, J. Fierrez Biometric antispoofing methods: a survey in face recognition IEEE Access, 2 (2014), pp. 1530-1552

[2]E. Marasco, A. Ross A survey on antispoofing schemes for fingerprint recognition systems ACM Comput. Surv., 47 (2) (2015)

[3]C. Sousedik, C. Busch Presentation attack detection methods for fingerprint recognition systems: a survey IET Biometr., 3 (4) (2014), pp. 219-233 [4]S. Marcel, S.M. Nixon, J. Fierrez, N. Evans Handbook of Biometric Anti-spoofing: Presentation Attack Detection Springer, Switzerland: Cham (2019) [5]L. Ghiani, D.A. Yambay, V. Mura, G.L. Marcialis, F. Roli, S.A. Schuckers Review of the fingerprint liveness detection (LivDet) competition series: 2009 to 2015 Image Vis. Comput., 58 (2017), pp. 110-128

[6]R. Agarwal, A.S. Jalal Presentation attack detection system for fake iris: a review Multimedia Tools and Applications, 80 (2021), pp. 15193-15214 https://www.indeed.com/career-advice/career-development/how-to-cite-a-research-paper

Thank You!