ENCRYPTION OF BIOMETRICS TRAITS FOR PRIVACY ATTACKS USING AES ENCRPYTION

A PROJECT REPORT

Submitted by,

Ms. Karen Rena C -20211CSD0169
Ms. Samprity Singha -20211CSD0044
Mr. Pavaman S Suraj -20211CSD0126

Under the guidance of,

Prof. Himansu Sekhar Rout

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING (DATA SCIENCE)

At

PRESIDENCY UNIVERSITY

BENGALURU

DECEMBER 2024

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

CERTIFICATE

This is to certify that the Project report **"Encryption of Biometrics Traits for Privacy Attacks using AES Encryption"** being submitted by "Karen Rena C, Samprity Singha, Pavaman S Suraj" bearing roll number(s) "20211CSD0169, 20211CSD0044, 20211CSD0126" in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering is a Bonafide work carried out under my supervision.

20/01/2025

Prof. Himansu Sekhar Rout
Assistant Professor
School of IS
Presidency University

20 Jan 25

Dr. Saira Banu Atham
Professor & HoD
School of CSE&IS
Presidency University

Dr. L. SHAKKEERA
Associate Dean
School of CSE
Presidency University

Dr. MYDHILI NAIR
Associate Dean
School of CSE
Presidency University

Dr. SAMEERUDDIN KHAN
Pro-VC School of Engineering
Dean -School of CSE&IS
Presidency University

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

DECLARATION

We hereby declare that the work, which is being presented in the project report entitled **Encryption of Biometric Traits for Privacy Attacks using AES Encryption** in partial fulfillment for the award of Degree of **Bachelor of Technology** in **Computer Science and Engineering**, is a record of our own investigations carried under the guidance of **Prof. Himansu Sekhar Rout, Assistant Professor, School of Information Science, Presidency University, Bengaluru.**

We have not submitted the matter presented in this report anywhere for the award of any other Degree.

Karen Rena C	**Samprity Singha**	**Pavaman S Suraj**
20211CSD0169	**20211CSD0044**	**20211CSD0126**

ABSTRACT

Biometric systems have become essential for secure authentication, utilizing unique traits such as fingerprints, iris patterns, and facial features. However, privacy concerns and vulnerabilities to attacks necessitate advanced methods for protecting biometric data. This project proposes a robust framework for encrypting biometric traits, combining multimodal biometrics, machine learning (ML), and the Advanced Encryption Standard (AES) to ensure both data confidentiality and authentication.

The system integrates iris and face biometrics, generating cryptographic keys through ML-driven feature extraction techniques from Pre-trained CNN models like VGG. These features are used to create a biometric key using Quantization which utilizes 16 bins, then converted to 256 byte key used in AES encryption for securing image data. Optimized AES implementations, including non-linear S-Box designs and Galois/Counter Mode, further enhance security and performance. Multimodal biometrics improve accuracy and resilience against spoofing attacks, addressing limitations of unimodal systems.

Research demonstrates that biometric-based key generation ensures unique and secure cryptographic keys while eliminating the need for traditional passwords. Machine learning enhances feature extraction and multimodal fusion, achieving high recognition accuracy. Combined with AES, this approach provides efficient, robust encryption resistant to brute force and spoofing attacks.

This framework addresses critical challenges like template instability, privacy risks, and computational overhead, making it ideal for real-world applications such as secure identity verification, data transmission, and access control. The integration of multimodal biometrics, ML, and AES represents a transformative step towards scalable, secure, and privacy-preserving authentication systems for the digital age.