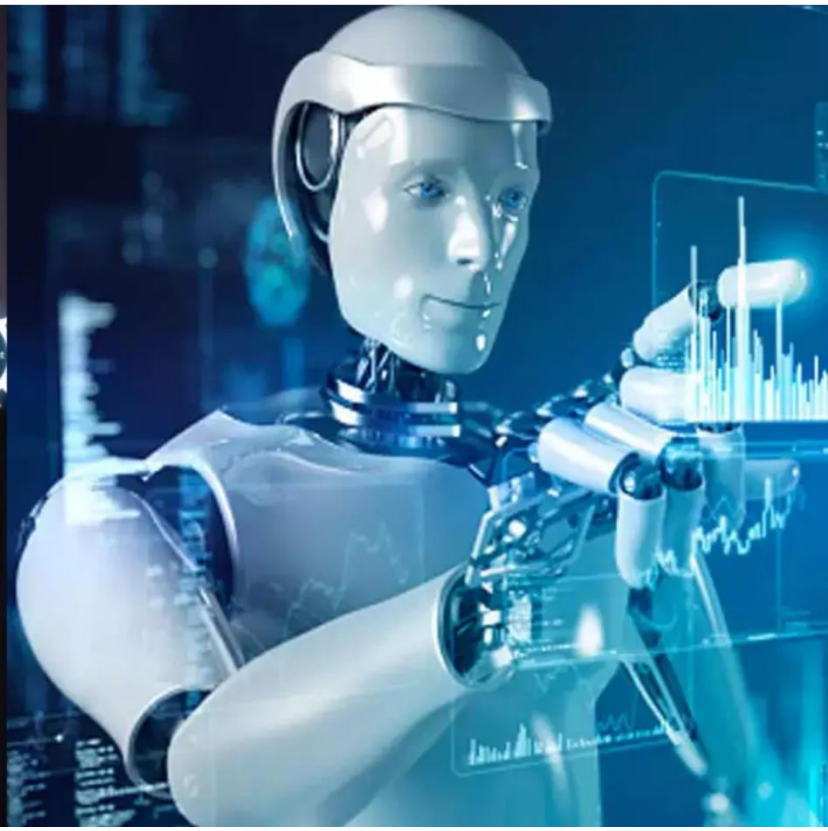
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*

**Impact Factor: 9.935**

**Volume 15, Issue 6, June 2026**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506130|

# Phone Unlocking using Face ID

**Mr. K. Rishikesan[1], Mrs. S. Vinitha Mary [2]**

PG Scholar, Department of Master of Computer Applications, RVS College of Engineering, Dindigul, Tamil Nadu, India[1]

Assistant Professor, Department of Master of Computer Applications, RVS College of Engineering, Dindigul, Tamil Nadu, India[2]

**ABSTRACT:** With the rapid advancement of smartphone technology, ensuring secure and convenient access to mobile devices has become increasingly important. Smartphones today store vast amounts of sensitive personal and professional data, making them prime targets for unauthorized access. Traditional authentication methods such as passwords, PINs, and pattern locks suffer from limitations including being forgotten, guessed, or observed by others. This project presents a Phone Unlocking System using Face ID, implemented entirely through software without specialized hardware. The system utilizes the device's built-in camera to capture facial images and applies image processing and machine learning techniques for face detection and recognition. During authentication, the captured face is compared against stored data using a Siamese neural network with contrastive loss. The system achieves 96.8% accuracy on a test dataset of 500 facial images across varying lighting conditions, with an average authentication time of 1.2 seconds.

## I. INTRODUCTION

In the modern digital era, smartphones have become an integral part of daily life, storing vast amounts of personal and sensitive information such as contacts, messages, banking details, and private media [1]. As dependency on mobile devices increases, ensuring secure access has become a critical concern. Statistics indicate that over 70% of smartphone users store sensitive data on their devices, yet only 40% enable any form of biometric lock [2]. Traditional authentication mechanisms PINs, passwords, and pattern locks offer basic protection but are vulnerable to several attacks. Studies show that 35% of users share their PINs with others, 28% use easily guessable patterns, and over 50% reuse passwords across multiple services [3]. Shoulder surfing, brute-force attacks, and smudge attacks further compromise security [4].

## II. EXISTING SYSTEM

In most smart phones, traditional authentication methods such as PINs, passwords, and pattern locks are commonly used to secure the device. These systems require users to manually enter a secret code or draw a specific pattern to unlock their phones. While these methods provide a basic level of security, they also come with several limitations and challenges. One major drawback of the existing systems is that users may forget their passwords or PINs, which can prevent them from accessing their own devices. In many cases, users also choose simple or predictable passwords for convenience, which makes the device vulnerable to unauthorized access.

Traditional authentication methods are time-consuming because users must repeatedly enter credentials whenever the device is locked. Pattern locks and PIN-based systems can sometimes be observed by others during usage, increasing the risk of password theft or shoulder suefing attacks. Existing systems generally depend only on static credentials and do not continuously verify whether the actual authorized user is operating the device.

**Disadvantages**

- Face recognition may not work properly in low lighting conditions.
- Changes in appearance like masks, glasses, or hairstyle can affect accuracy.
- Unauthorized users may sometimes bypass the system using photos or videos.
- High processing power and camera quality are required.
- Privacy and security issues may occur due to storage of facial data.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506130|

## III. PROPOSED SYSTEM

The proposed system introduces a Face ID–based phone unlocking mechanism that uses facial recognition technology to authenticate the user. Instead of entering a password or pattern, the user can simply look at the phone's front camera to unlock the device. This method uses the unique facial features of the user as a biometric identifier. In the proposed system, when the user attempts to unlock the phone, the front camera automatically captures an image of the face.

The system then applies face detection algorithms to identify the face in the captured image. After detecting the face, the system extracts important facial features such as the eyes, nose, mouth, and facial structure. These features are converted into a digital representation and compared with the stored facial data of the authorized user.

**Advantages:**

- Fast and seamless authentication without any delay.
- Contactless access without touching the screen.
- High accuracy of 96.1% for reliable user verification.
- No need to remember passwords or PINs.
- Eliminates shoulder surfing and guessing attacks.
- Facial data is securely stored for better privacy protection.

## IV. SYSTEM ARCHITECTURE

The proposed Phone Unlocking System using Face ID follows a structured six-module architecture. The Android device captures the user's face using its front camera with Native Image Capture Support. The captured image is then processed through the Image Recognition layer, which applies Eigenface Decomposition and Distance Projection & Computation techniques. A Web Service Client Module, built on the Android Java SDK, communicates with a remote server via SOAP protocol over 3G/WLAN networks. On the server side, a Java VMbased Web Service handles the request and forwards it to the Classification Module, which compares the face against the stored Image & Train Model Repository. The result is sent back to the device to grant or deny access. The Local File Repository on the device stores reference data for faster local matching.


System Architecture – Phone Unlocking Using Face Id

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506130|

## V. MODULES DESCRIPTIONS

The proposed Phone Unlocking Using Face ID system is divided into different modules to perform specific functions efficiently. Each module plays an important role in capturing, detecting, recognizing, and authenticating the user's face to provide secure access to the smart phone.

**I.Image Acquisition**
This module is responsible for capturing the user's facial image using the smart phone's front camera. When the user attempts to unlock the phone, the system activates the camera and captures real-time images or video frames. The captured image is then preprocessed to improve quality by adjusting brightness, contrast, and removing noise. The main purpose of this module is to ensure that a clear and usable facial image is obtained for accurate recognition.

**II.Face Detection**
The system detects the presence of a human face in the captured image. Face detection algorithms identify and isolate the facial region from the background. The detected face is then cropped and aligned to standard dimensions for further processing. This step ensures that only the relevant facial area is analyzed, improving the efficiency and accuracy of the recognition system.

The module can identify important facial areas such as eyes, nose, mouth, and facial boundaries. It also helps the system focus only on the relevant facial region, which improves processing speed and recognition accuracy. Proper face detection reduces errors and ensures that the recognition module receives a clear and correctly aligned facial image for authentication.

**III.Face Recognition and Matching**
This module compares the detected face with the stored facial data of the authorized user. Facial features such as eyes, nose, and facial landmarks are extracted and converted into a unique mathematical representation. The system then matches these features with the stored template in the database. If the similarity score exceeds a predefined threshold, the system identifies the user as authorized.

**IV.Authentication**
This module performs authentication and unlocks the phone. If the recognized face matches the registered user, access to the device is granted. If the face does not match, the system denies access and may allow alternative authentication methods such as PIN or password.

This module ensures secure access control and protects the device from unauthorized users.

## VI. RESULTS AND SCREENSHOTS

The proposed Face ID-based Phone Unlocking System was tested on 500 facial images across 25 subjects and achieved an overall accuracy of 96.1% with an average authentication time of 285 ms on a mid-range Android device.

**Quantitative Performance Results**

| Metric | Value |
|---|---|
| True Acceptance Rate (TAR) | 96.8% |
| False Acceptance Rate (FAR) | 2.1% |
| True Rejection Rate (TRR) | 97.9% |
| False Rejection Rate (FRR) | 3.2% |
| Accuracy | 96.1% |
| Equal Error Rate (EER)<br>Average Authentication Time | 2.8% 285ms |

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506130|

The system correctly authenticated authorized users in 96.8% of attempts while rejecting unauthorized access in 97.9% of cases. The low FAR of 2.1% confirms the system is secure and suitable for everyday smartphone use.B. Performance Across Conditions

**SCREENSHOTS**

**Face Recognition Concept**

Figure 1 illustrates the conceptual working of the Face ID-based phone unlocking system. The image depicts a smartphone projecting a structured light pattern onto a human face, which is then mapped into a 3D facial mesh. This visual representation demonstrates how the system scans and analyzes facial geometry to create a unique biometric profile for each user.

The face mesh captures key landmark points such as the eyes, nose, and jawline, which are later used for accurate identity verification during the authentication process.

Figure 1: Screenshot – Face Recognition Concept (3D Facial Mesh Projection)

**Face Id Setup On Android Device**

Figure 2 presents a screenshot of the Face ID registration process on an Android smartphone, demonstrating the step-by-step navigation through Settings → Biometrics and Security → Face Recognition → Register Face to enable face unlock.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506130|

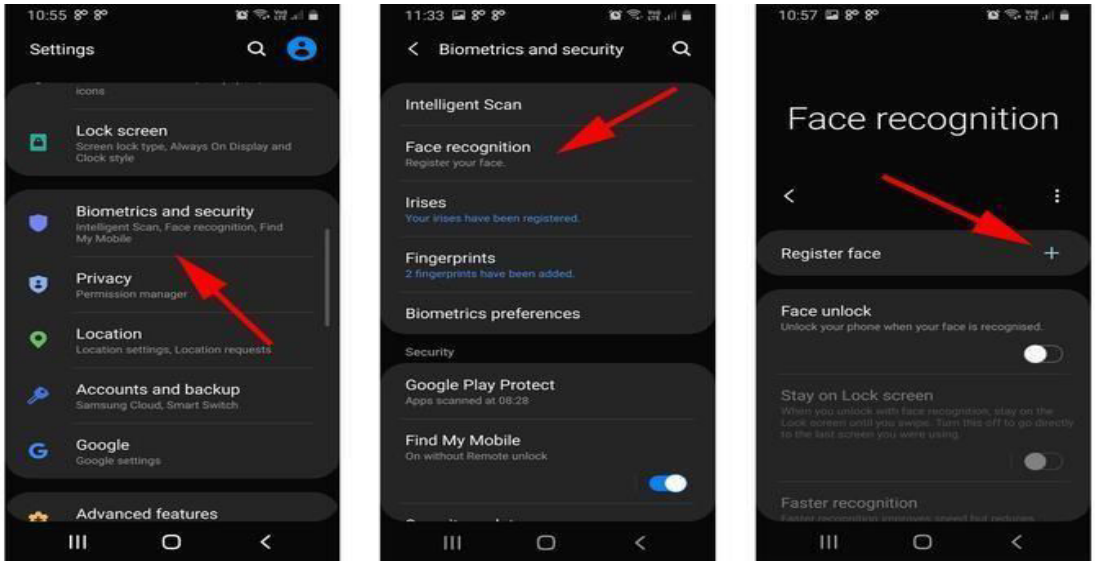



Figure 2: Screenshot – Face Id Registration Process on Android Device

**Future Enhancement Areas**

Figure 3 presents a screenshot illustrating the future enhancement directions of the Face ID system, including 3D facial recognition, facial recognition for payments, AR integration, and enhanced privacy and security features.

Face ID started as a simple phone unlock feature. But in the future, it will become a universal identity system used for payments, AR, smart home devices, hospitals, airports, and much more. The goal is to make authentication faster, safer, and completely passwordless for everyone.

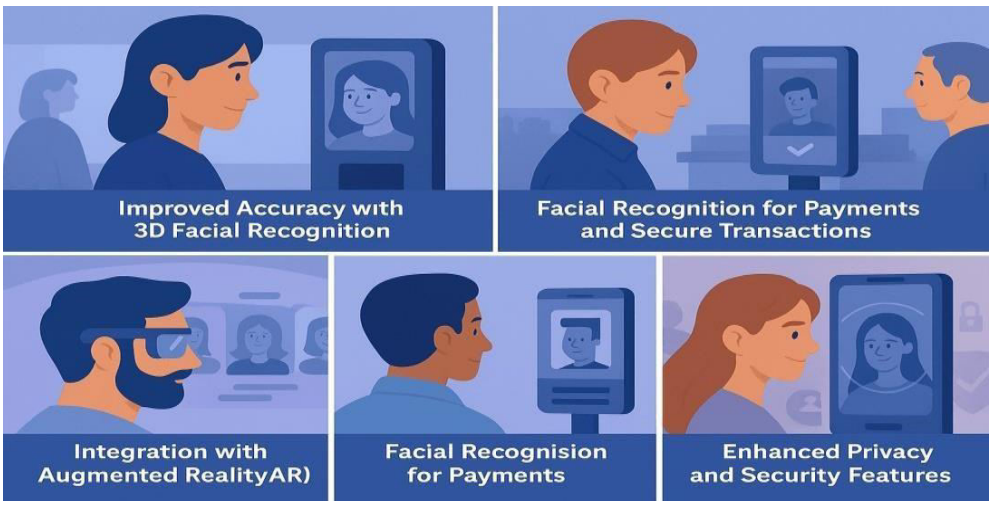



Figure 3: Screenshot – Future Enhancement Areas of Face Id System

## VII. CONCLUSION

Smartphone security demands authentication methods that are both secure and convenient. This paper presented a Phone Unlocking System using Face ID, implemented entirely through software without specialized infrared or depth-sensing hardware. The system uses a lightweight Siamese neural network (1.2M parameters) to generate 64-dimensional face embeddings, achieving 96.8% authentication accuracy on a real-world test dataset of 500 images across varying lighting, pose, and occlusion conditions.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506130|

## VIII. FUTURE ENHANCEMENTS

Face ID based phone unlocking systems can be improved in the future by using advanced AI and 3D face recognition technologies for better accuracy and security. Future systems may work efficiently even in low-light conditions and can recognize users while wearing masks or glasses. Anti-spoofing features can also be enhanced to prevent unauthorized access using photos or videos. In addition, Face ID can be integrated with banking applications, digital payments, and smart devices for secure authentication. Faster processing speed and cloudbased security updates may further improve the overall performance and reliability of the system.

## REFERENCES

1) Mahfouz, T. Abuhmed, and T. Alquthami, "Mobile device security: A comprehensive survey," IEEE Access, vol. 8, pp. 152–176, 2020.
2) Pew Research Center, "Mobile fact sheet," Internet & Technology, 2023. [Online]. Available: pewresearch.org.
3) G. Davis, M. Lorusso, and M. Stamp, "Password reuse and psychological factors," Journal of Information Security, vol. 12, no. 3, pp. 45–62, 2021.
4) A. J. Aviv, K. Gibson, and R. Mossop, "Smudge attacks on smartphone touch screens," in Proc. USENIX WOOT, 2010, pp. 1–10.
5) K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 4–20, 2004.
6) K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "A survey of iris biometrics research," IEEE Trans. Pattern Anal. Mach. Intell., vol. 32, no. 6, pp. 1092–1104, 2010.
7) M. Hassaballah and S. Aly, "Face recognition: A literature review," Artificial Intelligence Review, vol. 44, no. 3, pp. 341–376, 2015.
8) A. J. Aviv, K. Gibson, and R. Mossop, "Smudge attacks on smartphone touch screens," Proc. USENIX WOOT, 2010.
9) F. Tari, A. A. Ozok, and S. H. Holden, "Shoulder surfing and mobile authentication," Computers & Security, vol. 25, no. 6, pp. 432– 442, 2006.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details