RESEARCH ARTICLE OPEN ACCESS

IOT SECURITY PROTOCOLS FOR MULTIMODAL BIOMETRIC SYSTEM-BASED IDENTIFICATION OF INDIVIDUAL VAULT ACCESS

J Prashanthi[1] , T.Sai Santhoshi[2] ,K Rammohan Goud[3], Dr.Narasimha Chary Ch [4]

[1](Assistant professor, Dept of CSE
Sree Dattha Institute of Engineering and Science, Telangana)
[2](Assistant professor, Dept of CSE
Sri indu College of Engineering and technology (Autonomous)
Rangareddy District, Telangana 501510)
[3](Assistant Professor, Dept of CSE
St. Martins Engineering College, secunderabad -500100)
[4](Assoc.Prof.Dept of CSE
Sri indu college of Engineering and technology(Autonomous)
Rangareddy District-501510)

-------------------------------------*************************--------------------------------

Abstract:

This study proposes a PCA-based face and fingerprint recognition and authentication technique for IoT applications, enhancing efficiency and storage capacity. It uses user inputs, parallel matching, and multiple modalities for user authentication, emphasizing the importance of big data in businesses..

Keywords:- Biometrics with the Internet of Things: face, fingerprint, multimodal, security, and authentication

-------------------------------------*************************--------------------------------

I. Introduction

Biometric systems use human physiological or behavioral traits to verify identity. They function through enrollment and authentication, with biometric data collected and stored in a database. Authentication involves adding a user's identification to the biometric sample, while verification matches the user's biometric data to the database. Biometrics offer higher data security than passwords, using various types such as fingerprints, faces, iris, voice, signatures, and more.

Unimodal biometric systems face issues like noise, variability, and high error rates. Multimodal biometrics combine biometric data from multiple sensors, increasing recognition rate and overcoming limitations in unimodal systems.

Internet of Things (IoT)

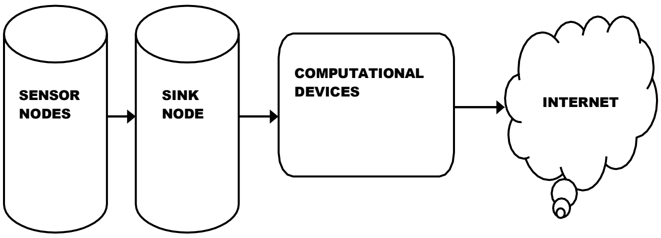


Fig.1: Architectural outline

II. Architecture Outline to Secure Io Using Multimodal Biometric System

The Internet of Things is crucial for securing personal data through biometric systems. These systems extract features from unique biometric traits, verify them, collect data, and store it for sharing and processing. Additional features can be added by adding more sensor nodes and using different biometric traits.

The Internet of Things (IoT) is a network of mechanical, biometric, and digital devices that enables Remote administration and data interchange. It captures the global market through digital transformation in computing and communication. Physical objects like people, sensors, and computers access the internet, enabling applications in physical space and cyberspace.

The Internet of Things has five domains [2] that allow devices to communicate with each other in various environments: the healthcare industry (tracking, identification/authentication, data collection, sensing), the transportation and strategy domains (logistics, assisted driving, mobile ticketing, environment monitoring), and the smart environment (comfortable homes and offices, industrial plants, smart museum and gym),

- Individual and communal domain (Social media, Past inquiries, Crimes, and losses);
- Prospective range (Autonomous vehicles, Urban data structure, Improved gaming area).

III. Fingerprint Biometric Concept

One of the earliest and most widely used biometrics for identity verification is the fingerprint. A person's thumb impression is their fingerprint. Handprints are distinct and inflexible. Applications for fingerprints include education, law, forensics, defense, mobile log-in, and license registration. These days, thermal, optical, silicon, and ultrasonic techniques are used to create fingerprint sensors. The orientation of the ridge ends and bifurcations, as well as other minute details, are used to identify fingerprints.

The following is a summary of fingerprint biometrics Benefits:

- A person's fingerprints remain the same throughout their entire life.
- High degree of uniqueness is established via fingerprints.
- The cost of fingerprint sensors is reasonable.

There are three primary phases involved in flawless fingerprint recognition.

First of them is fingerprint pre-processing.

2. Extraction of features

3. The Matching of Fingerprints print photos is ascertained

Pre-processing is a crucial initial step in enhancing the image's quality. During the feature extraction process, the image is thinned and its features are extracted. Fingerprint matching is the process of matching the input image to the enrolled image. The identification of the same finger between the two fingerprint pictures is determined at this phase. An essential first step in improving the image's quality is pre-Processing. The image is thinned and its features are extracted during the feature extraction process. Between the two finger

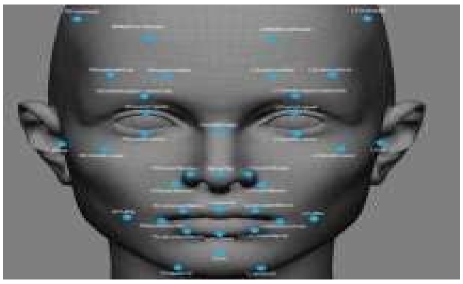


Fig. 3: Multimodal biometric fusion

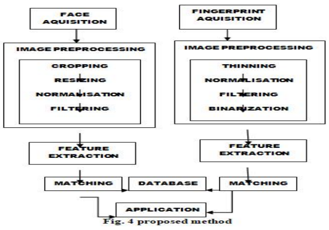


Fig. 4 proposed method

Cloud-enabled IoT and IoP will eventually be connected to one another. Research on human identification will become slower processing speed, smaller memory footprint, and worse precision, its reliability is reduced.

- value.

Face identification systems use nodal points, which are around 80 distinct facial traits. Sometimes distinctive characteristics are added as features, such as a mole or scar. Face biometrics' benefits are the hardware may be made inexpensively by using a simple camera to capture the image, and it can be utilized without the subject's knowledge. The drawbacks of face biometric Face identification and face resolution are the two stages of the face recognition system. Both phases use the same functional modules and methodologies. They are listed in the following order:

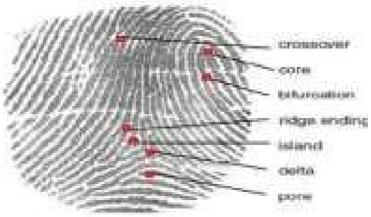


Fig. 2: biometric fingerprint and face

The biometrics is combined in the figure below to calculate the score value. If the score value is maximum,

the user is considered authorized; if the score level is below

the threshold, the user is considered unauthorized.. increasingly important for identity authentication, data access, and information privacy.

The biometric authentication method using the fingerprint and face is more successful in enhancing security. There are now two types of biometric identification methods available: multimodal biometric identification using two fully unimodal systems and unimodal biometric identification. A unimodal biometric system has a classifier and feature extractor of its

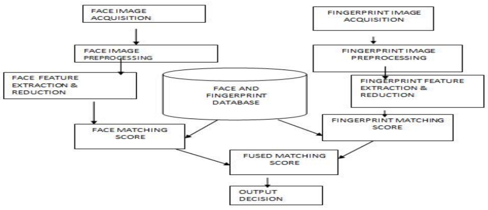
- Image acquisition and detection: This module uses any camera to take a picture of the user's face, then filters out any areas that aren't needed for face identification to only collect the portion of the face that is utilized for face identification.
- Image pre-processing

Pre-processing techniques like thinning, grayling, and normalization are used to improve the image when the quality of the facial image is not up to par.

- Matching and extracting features:

face features are extracted and compared with all of the enrolled face features kept in the database using a feature extraction technique. The matching module states that it has two.

IV.Proposed Methodology


FACE IMAGE ACQUISITION
FINGERPRINT IMAGE ACQUISITION
FACE IMAGE PREPROCESSING
FINGERPRINT IMAGE PREPROCESSING
FACE FEATURE EXTRACTION & REDUCTION
FACE AND FINGERPRINT DATABASE
FINGERPRINT FEATURE EXTRACTION & REDUCTION
FACE MATCHING SCORE
FINGERPRINT MATCHING SCORE
FUSED MATCHING SCORE
OUTPUT DECISION

The suggested strategy uses a fusion-based multimodal biometric identity system to automate personal vault security. Face and fingerprint are employed as the biometric database in this procedure. In order to reduce the likelihood of hacking, two biometric features are combined. A schematic representation of the proposed system's foundation can be found in Figure 4.
The user uses his or her gadget to provide input to the internet. Verification of the fingerprint and facial inputs is carried out online.. After the verification of the details about the user, the system passes on the signal for the vault to open.

Because it offers more security than the current approaches, the suggested plan is superior. Fig. 4 displays the block diagram for the suggested methodology. In essence, the matcher obtains and approves the user's fingerprint as the first input, then obtains and verifies the user's face as the second input. The combination of both biometrics completes the process. Figure 5 depicts the suggested fusion-based multimodal biometric. The suggested strategy uses less memory, a simple design, faster processing, strong security, and enhanced processing speed to increase system effectiveness.

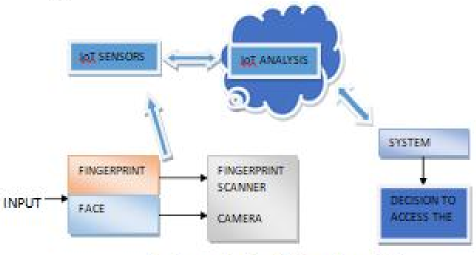


Fig. 5Proposed multimodal biometric methodology

VI. Conclusion

In this study, we build very high efficiency and performance by merging the features of fingerprint and face. The main benefit of this multimodal biometric authentication is that it uses very little memory and inexpensive hardware and software. The suggested strategy can be applied in domains including internet payment, defense, and migration verification where a high level of security is desired. This study describes a very low-cost, low-storage-space computing technique. All smartphones have a high-quality camera, which is all that is needed for this method to work, allowing any user to identify them with just one picture. Future efforts will concentrate on enhancing security protocols and utilizing biometrics to protect individuals' privacy.

VII. References

1. Sujatha, K., Pappa, N.: Combustion monitoring of a water tube boiler using a discriminant radial basis network. ISA Trans. 50, 101–110 (2011).

2.Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey.Computer networks, 54(15), 2787-2805.

3. Chary, D. C. N., Babu, M. R., & More Sadanandam, S. K. (2023). Leveraging Deep Learning Techniques For The Stability Principles Of Current Artificial Neural Networks Are Emerging Into Their Activation Functions.

4. Ch, N. C., Chintha, S., Rajendra, E., & Srinivas, S. Generalized Flow Performance Analysis Of Intrusion.

5. Detection Using Azure Machine Learning Classification CH, N. C., Navya, B., Chintha, S., & Nagu, K. Big Data in Healthcare Systems and Research.

6. Ch, D. (2021). Narasimha Chary,”. Comprehensive Study On Multi-Operator Base Stations Cell Binary And Multi-Class Models Using Azure Machine Learning”," A Journal Of Composition Theory, 14(6).

7. Vijayajyothi, C., & Srinivas, D. (2023). Abnormal Activity Recognition In Private Places Using Deep Learning.". International Journal Of Computer Techniques, 10(2), 1-11.

8. Chary, D. C. N., Babu, M. R., & More Sadanandam, S. K. (2023). Leveraging Deep Learning Techniques For The Stability Principles Of Current Artificial Neural Networks Are Emerging Into Their Activation Functions.

9.Ch, N. C., Chintha, S., Rajendra, E., & Srinivas, S. Generalized Flow Performance Analysis Of Intrusion Detection Using Azure Machine Learning Classification.

10. Chary, C. N., Krishna, A., Abhishek, N., & Singh, R. P. (2018). An Efficient Survey on various Data Mining Classification Algorithms in Bioinformatics. International Journal of Engineering and Techniques, 4

12. Chary, D. C. N., Babu, M. R., & More Sadanandam, S. K. (2023). Leveraging Deep Learning Techniques For The Stability Principles Of Current Artificial Neural Networks Are Emerging Into Their Activation Functions.

13. Shobarani, R., Sharmila, R., Kathiravan, M. N., Pandian, A. A., Chary, C. N., & Vigneshwaran, K. (2023, April). Melanoma Malignancy Prognosis Using Deep Transfer Learning. In 2023 International Conference on Artificial Intelligence and Applications (ICAIA) Alliance Technology Conference (ATCON-1) (Pp. 1-6). IEEE.

16.Ch, N. C., Chintha, S., Rajendra, E., & Srinivas, S. Generalized Flow Performance Analysis Of Intrusion Detection Using Azure Machine Learning Classification.

17.Ravi, C., Cholleti Narasimha Chary, D., Raju, M. B., & Srinivas, S. Analysis Of Concept Drift Detection–A Framework For Categorical Time Evolving Data.

11.Vijayajyothi, C., & Srinivas, D. (2023). Abnormal Activity Recognition In Private Places Using Deep Learning..". International Journal Of Computer Techniques, 10(2), 1-11.

14. Chary, D. C. N., Babu, M. R., & More Sadanandam, S. K. (2023). Leveraging Deep Learning Techniques For The Stability Principles Of Current Artificial Neural Networks Are Emerging Into Their Activation Functions.

15. Vijayajyothi, C., & Srinivas, D. (2023). Abnormal Activity Recognition In Private Places Using Deep Learning..". International Journal Of Computer Techniques, 10(2), 1-11.