Computer Science Department

Computer Security (COMP432)

Project Report

Electroencephalography (EEG) Biometrics "Brain Waves Biometric"

Student's names	Student's numbers
Rayan Ghnimat	1211073
Ahed Ghnimat	1201849
Ameer Qadadha	1221147

Instructor: Hafez Barghouthi

Contents

Table of figure

Table of Table

Abstract:

As technology improves, keeping our personal information safe is more important than ever. Common security methods like passwords, fingerprints, and face scans are no longer enough because hackers can find ways to break them. This report looks at a new and more secure method called brainwave biometric identification. It uses a technology called Electroencephalography (EEG) to measure brainwaves, which are patterns created by the brain. These patterns are different for every person, making them very hard to copy or fake. This report explains how brainwave identification works, why it is more secure than older methods, and how it could be used in the future to protect sensitive information.

Chapter 1: Literature Review

1.1 Introduction

Security is no longer optional—it's necessarily. With the increase of cyber threats, protecting personal data and sensitive information has been harder throughout time. As technology evolves, so do the methods of authentication and identification. From passwords and PINs to fingerprints and facial recognition, each method offers its own level of security. However, all of these techniques have been broken or corrupted by modern hacking methods.

This report comes out with the most advanced idea in the field of security: brainwave biometric identification. It simply uses Electroencephalography (EEG) that helps to measure the unique pattern of brainwaves. This help because brainwaves patterns are unique to each person, this technology offers a highly secure and nearly impossible to corrupt method of verifying identity.

1.2 Discussion

Here we examine how brainwave biometrics may be considered as a powerful substitute for current common biometric methods such as fingerprint scanning and facial recognition. It highlights the fact that brainwave signals are distinct for every person, making them a complete, secure and unique option for enhancing security in identity authentication systems.

Even if both brainwaves' patterns are unique and so are the fingerprints, but the main difference is that fingerprints have now specific techniques to be corrupted, just like using an object the person touched and then using specific devices to extract the pattern of the fingerprint then using it to open any type of information that is secured with that fingerprint. However, with the brainwave's patters, you need sensors and specific device.

You surely can't invent something without facing challenges and obstacles. Many challenges will be faced to make this feature achievable, just like expensive equipment, changing brainwaves because of the person's mood, technical accuracy and many other challenges. However, when you're facing challenges, you know that you're actually on the right way, So, achieving this will definitely be hard but it is not impossible.

Chapter 2: Biometrics Overview

2.1 Biometrics Definition

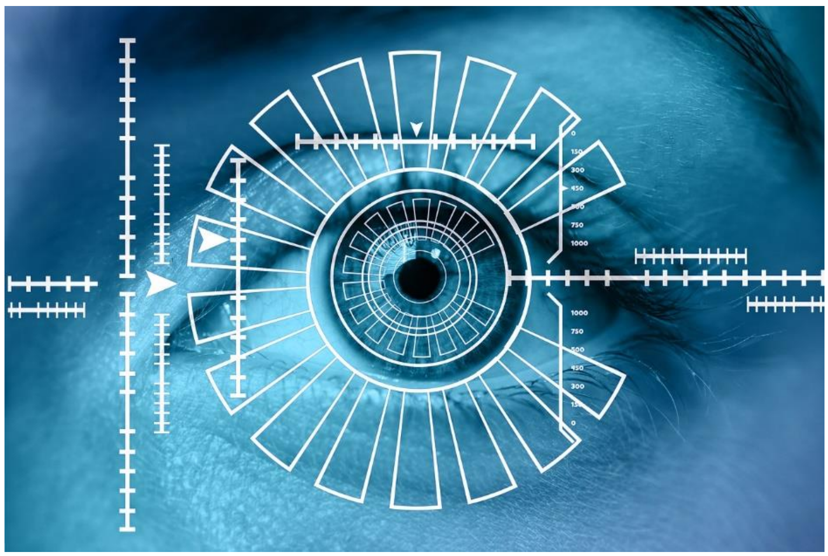

Figure 1:Biometrics

Biometrics refers to the use of unique physical or behavioral characteristics to identify individuals. These traits can include things like fingerprints, iris patterns, facial features, voice, and even behavioral traits such as gait (how someone walks). Biometrics has become a powerful tool in many industries for providing secure, accurate, and efficient identity verification[1].

2.2 Types of Biometrics:

1. **Physiological Biometrics:**
   This type relies on **physical characteristics** that are unique to each person. Common examples include:
   - **Fingerprints** – The ridges and patterns on your fingers.
   - **Iris Scans** – The unique patterns in the colored part of your eye.
   - **Facial Recognition** – Analyzing the distinctive features of your face.
2. **Behavioral Biometrics:**
   This type focuses on **how people act**, as these behaviors are also unique to individuals. Examples include:
   - **Voice Recognition** – Identifying someone based on their voice patterns.
   - **Signature Recognition** – Verifying identity based on the unique way someone signs their name.
   - **Gait Recognition** – Recognizing someone by how they walk.
3. **Neural Biometrics:**
   This advanced method uses the **brain or heart's activity** for identification. Some examples are:
   - **EEG (Electroencephalography)** – Identifying patterns in brainwaves.
   - **ECG (Electrocardiogram)** – Identifying patterns in the heart's electrical activity.

2.3 Advantages of Biometrics:

- **High Security:** Biometric data is unique to each person, making it hard to forge or steal.
- **Convenience:** It allows for **quick** and **easy** identity verification without needing passwords or physical cards.
- **Accuracy:** Biometric traits are reliable and precise for identification.
- **Non-repudiation:** Since biometrics are tied to an individual, they can't easily deny actions taken using their identity.

Chapter 3: Brainwaves Overview

3.1 Brainwaves Definition

Brainwaves are oscillating electrical voltages in the brain measuring just a few millionths of a volt. There are five widely recognized brain waves, and the main frequencies of human EEG waves. They are produced by synchronized electrical pulses from masses of neurons communicating with each other. Their speed is measured in Hertz (cycles per second) and they are divided into bands delineating slow, moderate, and fast waves[3].

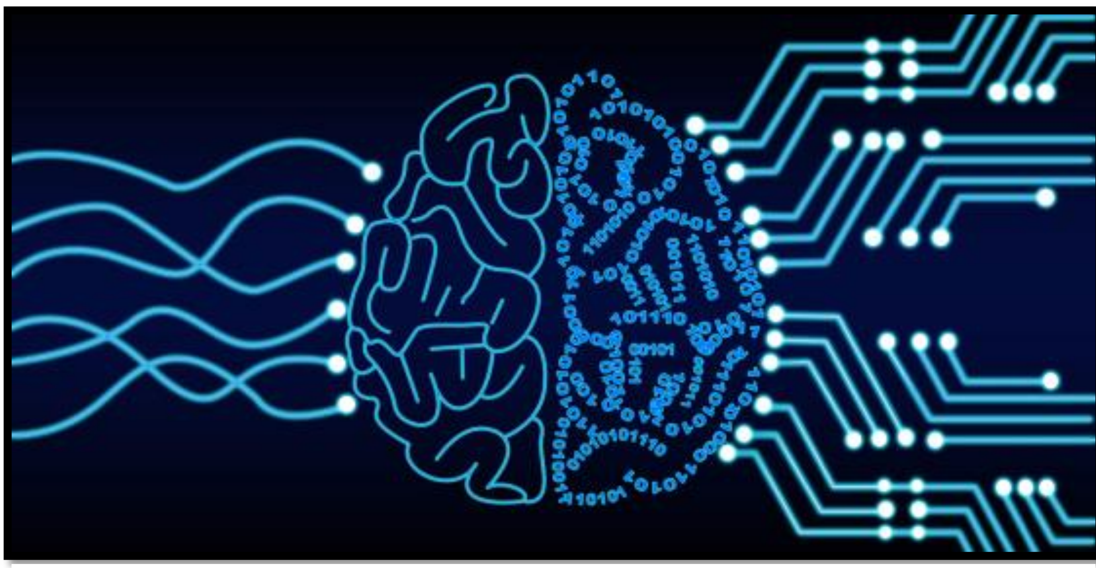

Figure 2: Brainwaves

3.2 Types of Brainwaves:

The electrical activity in the brain depends upon the type of activity being done by a person. These brain waves/rhythms are classified in five categories, and provide information about a person's health and state of mind. The categories are described in the following subsections. The five categories are[2]:

3.2.1 Gamma Waves (γ):

A gamma wave is considered to be the fastest brain activity. It is responsible for cognitive functioning, learning, memory, and information processing. Prominence of this wave leads to anxiety, high arousal, and stress, whereas it lacks can cause attention deficit hyperactivity disorder (ADHD), depression. Its frequency is in the range of (30Hz and above).

3.2.2 Beta Waves (β):

Beta waves are involved in conscious thought and logical thinking, and tend to have a stimulating effect, having the right amount of beta waves allows us to focus. Prominence of this wave causes anxiety, high arousal, an inability to relax, and stress, whereas its suppression can lead to ADHD, daydreaming, depression. Its frequency is in the range of (16-30Hz).

3.2.3 Alpha Waves (α):

An alpha wave helps us calm down when necessary and promote feelings of deep relaxation. They are found in daydreaming, inability to focus, and being very relaxed. If they are suppressed it can cause anxiety, high stress, and insomnia. Its frequency is in the range of (8-15Hz).

3.2.4 Theta Waves (θ):

This particular frequency range is involved in daydreaming and sleep. When theta waves are prominent it can cause depression, ADHD and impulsivity. Theta waves have benefits of helping to improve our intuition and creativity, and making us feel more natural. Its frequency is in the range of (4-7Hz).

3.2.5 Delta Waves (δ):

Delta waves are the slowest recorded brain waves in human beings. They are found most often in infants and young children, and are associated with the deepest levels of relaxation. They are seen in brain injuries, learning problems, inability to think. Its frequency is in the range of (0.1-3Hz).

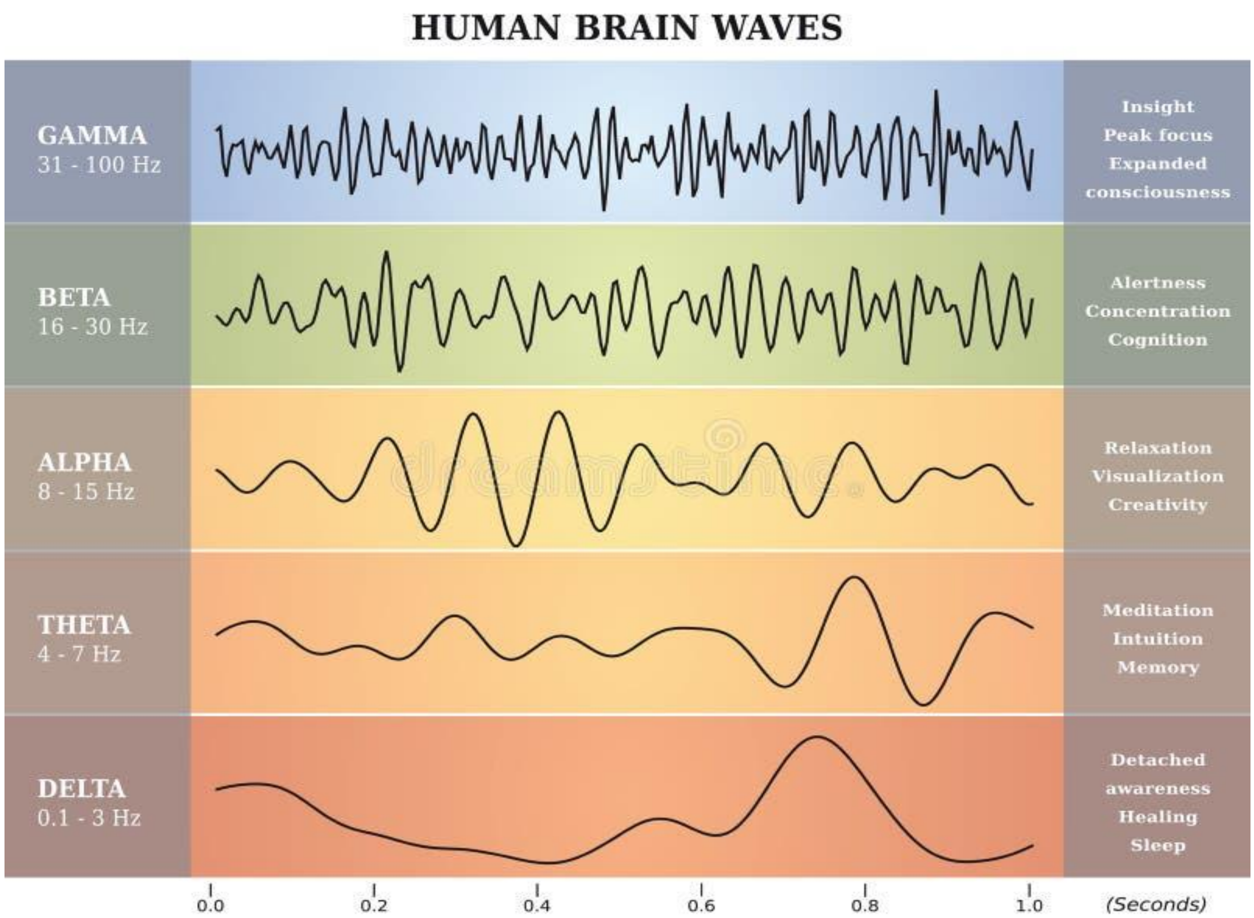

Figure 3: Brainwaves

Chapter 4: EEG

4.1 What is EEG:

EEG (Electroencephalography) is a non-invasive technique used to measure electrical activity in the brain. It captures the brain's electrical impulses by placing electrodes on the scalp. The data gathered reflects the brain's rhythmic patterns, called brainwaves, which vary according to mental states, such as being awake, relaxed, stressed, or asleep[4].

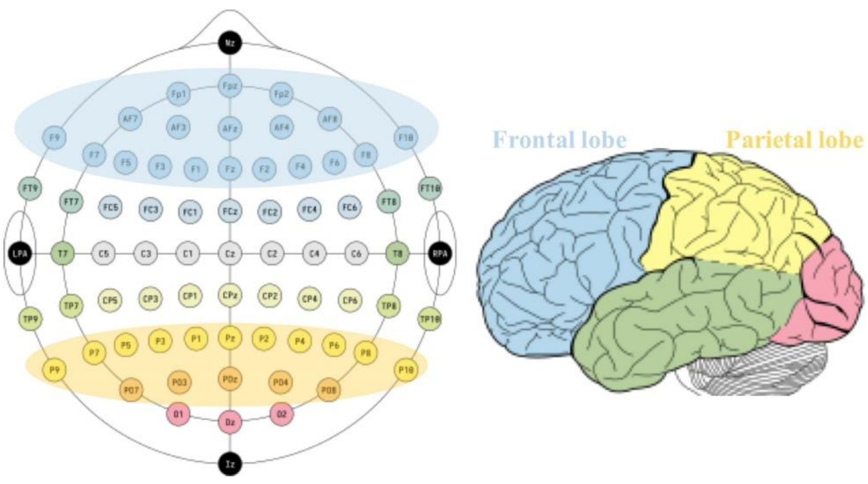

Figure 4: What is EEG

4.2 Functionality of EEG:

1. **Neural Activity in the Brain**:
   The brain consists of billions of neurons that communicate through electrical impulses. These neurons generate electrical activity when performing various tasks, such as thinking, moving, or even while sleeping. These electrical signals create **brain waves**, which vary depending on the brain's activity (e.g., focus, relaxation, or sleep).
2. **Electrode Placement**:
   Small sensors called **electrodes** are placed on the **scalp**. These electrodes detect the electrical signals from the brain. The electrodes are positioned using a standard system called the **10-20 system**, which covers specific areas of the scalp, ensuring all key brain regions are monitored.
3. **Signal Detection**:
   The electrodes pick up weak electrical signals from the brain, typically ranging from **1 to**

100 microvolts. These signals are too faint to be seen without specialized equipment, so they are amplified using the EEG machine to make them readable and analyzable.

4. **Recording and Display**:
   After amplification, the signals are sent to a computer or EEG machine, where they are recorded and displayed on a **monitor** as **brain wave patterns**. These patterns show the **frequency** (speed) and **amplitude** (strength) of the brainwaves.

5. **Analysis and Diagnosis**:
   The recorded data is analyzed by specialists to evaluate brain activity patterns. Abnormalities in brainwaves, such as those seen in **epileptic seizures**, **sleep disorders**, or **brain injuries**, can be detected, helping with diagnosis and treatment planning.

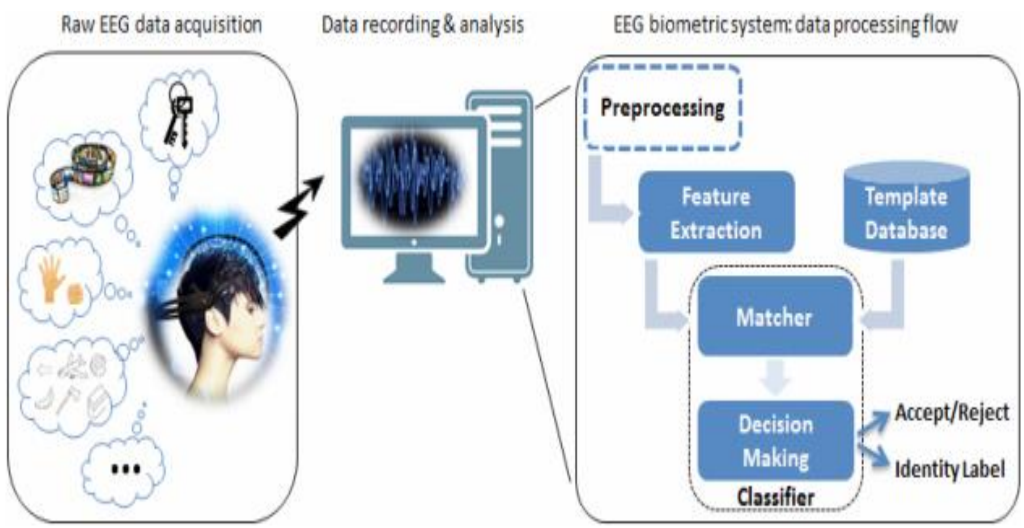

Figure 5: Functionality of EEG

4.3 EEG vs Other Biometric Tools

EEG (Electroencephalography) stands out as a biometric tool for several key reasons[5]:

1. **Uniqueness & Security:** EEG signals are unique to each person, just like fingerprints or facial recognition — but much harder to fake. While fake fingerprints or photos can trick traditional systems, EEG patterns require the actual person's cooperation and mental state, making them extremely difficult to replicate or spoof.
2. **Enhanced Security & Accuracy:** Unlike fingerprints or facial scans that can be copied or forged, EEG data is highly resistant to attacks. Even if someone steals the data, reproducing the brain's activity without the real person is nearly

impossible. Plus, EEG systems can continuously check if the user is still present, offering ongoing authentication for stronger security.

Chapter 5: Challenges of EEG Biometrics

Table 1:Challenges of EEG Biometrics

Challenge	Sub-Challenge	Description
Accuracy and Signal Quality	-Noise and Artifacts - Signal Variability	-Noise and artifacts affect signal accuracy. - Variations in brainwaves due to mental state, fatigue, or stress.
Environmental Interference	- External Factors - Controlled Testing Environments	-Electromagnetic interference distorts signals. - Requires controlled environments for accurate readings.
User Cooperation	- Active Participation - Variability in Mental States	- Requires user to stay still and engage in tasks. - Mental affects.

Chapter 6: Brainwaves Biometrics Progress

6.1 Milestones:

- **First Human EEG Recording:**

  In 1924, German physiologist Hans Berger records the first human electroencephalogram (EEG), laying the foundation for measuring brainwave activity, expanding on work previously conducted on animals by Richard Caton and others, Berger also invented the electroencephalograph. This was the first step of creating and understanding the concept of EEG[6].

- **Postmortem EEG Signals:**

  In 2022, for the first time in history, EEG signals of a deceased person were successfully captured, in addition, it is found that EEG-based authentication literature did not completely implement “liveness detection.”

- **A Large-Scale, Multi-Session Evaluation:**

  In 2025, The field of brainwave-based biometrics has gained attention for its potential to revolutionize user authentication, a large study was conducted using a public brainwave dataset of 345 subjects and over 6,000 sessions. The results reveal the Equal Error Rate (EER) increased over time—from 7.7% after one day to 19.69% after a year.

6.2 Potential Impact

1. **Unmatched Security**:

   Impossibility of replication: As brainwave patterns are unique to each individual, this system offers an exceptionally high level of security. Even if a hacker gains access to a person’s EEG data, it is nearly impossible to replicate or forge their brainwave patterns with the same precision.

2. **Economic Impact**:

   High implementation cost: Although brainwave authentication provides exceptional security, the cost of EEG equipment and the need for infrastructure updates may prevent many organizations from adopting this technology on a large scale.

6.3 Future Developments in Brainwave Biometrics (EEG)

- **Better Accuracy**: As machine learning and AI improve, brainwave identification will become more precise, making it more reliable and harder to trick.
- **Combining with Other Biometric Systems**: EEG will be used alongside other biometric methods like fingerprints, facial recognition, and voice to provide even more secure identity verification.
- **Brain-Computer Interfaces (BCIs):** Brainwave biometrics will connect with BCIs, allowing us to control devices and interact with technology just by thinking, making the process seamless for both authentication and user interaction.

How AI Enhances Brain Wave Applications:

AI is transforming the way we analyze and utilize brainwave data. By using machine learning, AI can process brainwave patterns with higher accuracy than humans. Here's how AI is improving brainwave technology:

1. **Real-time Analysis**: AI can instantly analyze brainwave data to detect mental states like focus, relaxation, or stress. This allows for immediate feedback.
2. **Brain-Computer Interfaces (BCIs)**: AI decodes brainwaves to enable direct interaction with devices using only thoughts. This helps people with physical disabilities control prosthetics[7].

6.4 EEG and IoT Integration: Real-World Examples

The integration of **EEG (Electroencephalography)** with **IoT (Internet of Things)** devices is transforming various aspects of daily life and healthcare. For example, wearable EEG devices, such as headbands that measure brain activity, can be connected to **smart home systems**. These systems adjust the environment based on real-time brainwave data—if the EEG detects stress or fatigue, the IoT system might dim the lights, play calming music, or adjust the room temperature to create a more relaxing atmosphere. In healthcare, IoT-enabled EEG devices are used for **epilepsy monitoring**; if a seizure is detected through abnormal brain activity, an alert is sent to caregivers or medical professionals, ensuring prompt assistance. Additionally, in **brain training**, EEG devices can track a person's cognitive state and send feedback to a connected IoT platform, which then guides users through **neurofeedback exercises** to improve focus, reduce anxiety, or enhance mental performance. Finally, **smart sleep monitoring** is another area where EEG and IoT come together—an IoT-enabled EEG system can track sleep patterns, adjust room conditions for better rest, and help users improve their sleep quality. These examples demonstrate the powerful potential of combining EEG with IoT for a more personalized and responsive experience[8].

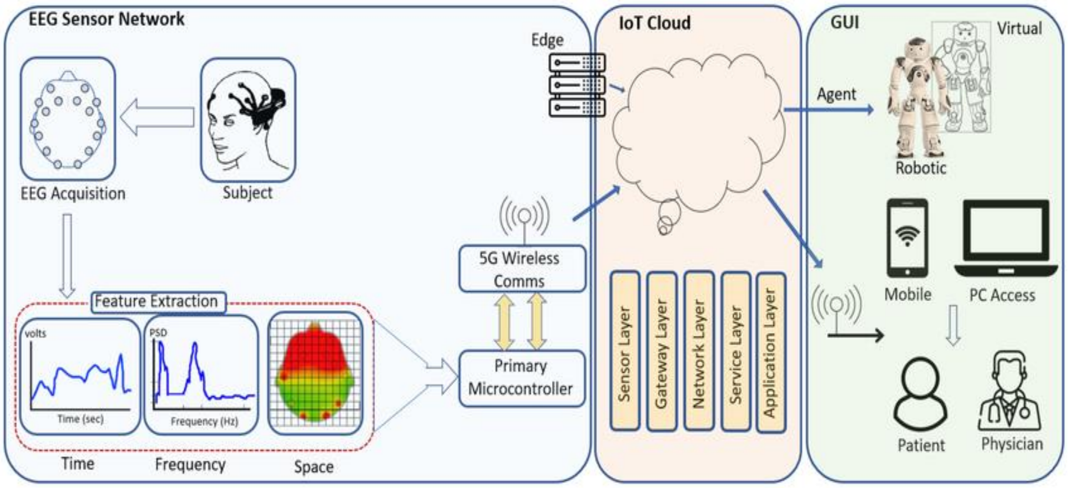

Figure 6:EEG and IoT Integration

Conclusion

As cybersecurity keeps getting more complicated, the need for better and safer ways to confirm someone's identity becomes more important. This report looked at how EEG-based biometrics can help. Unlike passwords, fingerprints, or face scans, EEG uses brainwaves, which are unique to each person and very hard to hack. By reading these brainwave patterns, EEG gives a more secure and reliable way to identify people. There are still some challenges like cost, signal quality, and differences between users, but progress is being made. Also, using EEG with smart devices (IoT) brings new ideas for healthcare, smart homes, and controlling devices with the mind. In the end, EEG biometrics could become a strong and easy way to keep things safe in the future.

References:

1. Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to Biometrics*. Springer Science & Business Media.
2. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2003). *Handbook of Fingerprint Recognition*. Springer Science & Business Media.
3. Niedermeyer, E., & da Silva, F. L. (2004). *EEG Signal Processing*. Elsevier.
4. Niedermeyer, E., & da Silva, F. L. (2004). *Electroencephalography: Basic Principles, Clinical Applications, and Related Fields*. Lippincott Williams & Wilkins.
5. He, H., & Wu, D. (2017). "Transfer Learning for Brain-Computer Interfaces: A Euclidean Space Data Alignment Approach". *IEEE Transactions on Biomedical Engineering*.
6. Liu, X., & Sourina, O. (2008). *Real-time Brainwave Monitoring for Mental State Estimation*. In *Proceedings of the International Conference on Cyberworlds*.
7. Lee, S., Kim, H., & Yoon, J. (2020). "Recent Advances in Brain-Computer Interfaces: From Medical Applications to Augmented Reality". *IEEE Transactions on Biomedical Engineering*.
8. Lee, J. H., Kim, H., & Park, J. (2016). "IoT-Based Wearable Healthcare Systems". *Sensors*.