Mindlock: Utilizing Convolutional Neural Network and Support Vector Machine for Brainwave-based Authentication

In the Partial Fulfillment of the
Requirements of CSRP 1

By
Amante, Vehuel M.
Asuncion, Lance S.
Eullo, Don Daniel M.
Oyama, Ryu L.

November 2024

Table of Contents

LIST OF FIGURES AND TABLES

Abstract - **With the increasing demand for a secure authentication method, this study introduces a brainwave-based biometric system using electroencephalography (EEG). This study takes advantage of the user's reaction to a task stimulus which is proven to be distinct and suitable as a biometric factor [10], [11], [12]. Convolutional neural networks as feature extractor and support vector machine for classification were used in this study. Using M3CV dataset which includes two sessions, the model achieved an accuracy of 97.12%, false acceptance rate (FAR) of 0.75% and false rejection rate (FRR) of 2.88% indicating the model's ability to accept registered users and reject intruders. Session 2 produced an accuracy of 49.86%, FAR of 0.69% and FRR 50.14% which highlight the need for improvements in the CNN-SVM model to ensure consistent performance across sessions.**

Keywords - **electroencephalography, event-related potential, M3CV, brainwave-based authentication**

CHAPTER I

INTRODUCTION

A. Background of the Study

In the digital realm, making sure that sensitive information can be accessed securely is very important. Current security processes include encryption protocols and firewalls, among others play a pivotal role in securing user data while reducing risks of unauthorized access or any form of data breach [1]. However, as technology keeps changing so does the tactics used by malicious actors which compels continuous authentication innovation.

User verification protocols are built on common authentication methods such as passwords, two-factor authentication (2FA), and biometrics. The ubiquity of passwords as a means of authenticating notwithstanding, their susceptibility to brute-force attacks and phishing exploits highlights the need for more security layers [2]. Additionally, two-factor authentication requires users to provide secondary verification that is usually in the form of a code sent through a text message or email [2]. However, biometric identification uses features such as fingerprints and facial recognition to verify a user's identity which provides a stronger and more convenient method of authenticating oneself [3].

Common vulnerabilities still exist despite the advancements made in the authentication technology which are considered dangerous to users. These weaknesses result from different factors including knowledge-based vulnerability where users unintentionally expose sensitive information and biometric vulnerability which is caused by potential limitations of biometric traits [7]. Also, traditional authentication techniques are prone to be exploited because they have their limitations such as being easily stolen, lost or duplicated[7].

To provide secure and reliable user verification, biometric authentication systems present an interesting option instead of the traditional approaches making use of inherent distinctions in organic characteristics. By identifying individuals accurately through physiological or behavioral traits, biometrics eliminate the need for passwords and cut the risk of unauthorized access [4]. Despite being a significant leap forward in security technology, biometric authentication still has its drawbacks. This calls for more sophisticated authentication solutions as traditional biometric systems can still be defeated by spoofing or forgery [3].

EEG brainwave authentication is described as an innovative method based on electroencephalography (EEG) that identifies users' unique brainwave patterns [5]. Contrary to conventional biometrics relying on physical qualities, Brainwave authentication is a more dynamic and intrinsically secured way of verifying the users [5]. By studying brainwave changes due to stimulations to authenticate people differently from existing methods with respect to reliability and safety [5].This innovative approach not only enhances security but also offers a seamless, user-friendly method of verifying identity, showcasing the potential of integrating neuroscience with cybersecurity to redefine traditional security measures [6]. Brainwave authentication overcomes the shortcomings of traditional methods through revolutionizing cyber-security paradigms with its seamless yet highly secure verification process for users. The study aims to bring about a more robust and user-centric approach towards cybersecurity in the digital age through this inquiry.

Brainwave authentication represents an innovative approach to enhancing authentication systems by analyzing an individual's brain activity patterns. This method utilizes EEG technology, commonly employed in medical fields for scanning and observing brain activity related to conditions such as epilepsy and sleep disorders [8]. In the context of authentication systems, EEG captures brain activity, which is then processed by algorithms to recognize unique patterns associated with specific individuals.

By leveraging the distinctive characteristics of EEG signals, brainwave authentication offers several advantages over traditional biometric methods. Unlike static biometric features, brainwave patterns are dynamic and difficult to replicate, ensuring robust security measures. Additionally, EEG authentication requires the subject to be alive, adding an extra layer of authentication integrity.[13] Therefore, biometric authentication using brainwaves has a series of advantages when compared to other biometric methods. Research on biometric authentication using an electroencephalogram (EEG) has already been carried out from various fields, and it has been clarified that it shows distinctive characteristics depending on the individual [13]. The studies on brainwave authentication systems [16], [10], [3], collectively provide insights into the feasibility and effectiveness of EEG-based authentication methods.

EEG-based authentication systems require specialized hardware devices to capture brain activity effectively. For instance, helmets or caps with metal sensors are commonly used to pick up electrical signals in the brain [9]. These signals are then cleaned and processed to extract relevant features that can be used for authentication purposes. Research indicates that EEG readings exhibit significant variability between individuals due to factors such as genetics, physiology, and overall health. Each person's brain processes billions of neurons, leading to unique responses to stimuli. Studies have highlighted the individuality of brainwave patterns, emphasizing how genetic and experiential factors shape EEG readings [10], [11], [12].

Research shows that everyone's brain waves are different because of things like genetics, how their body works, and overall health. [10] explains that since each person's brain has billions of nerve cells, they respond uniquely to information. Another study [18] adds that our DNA also affects how our brains are built, which then influences how we react to things based on our experiences. [19] mention that what we see and hear can also affect how our brains work and contribute to these differences. So, basically, our brainwaves are like fingerprints, unique to each person, shaped by both our biology and our experiences.

The association of alpha waves with mental relaxation suggests the efficacy of techniques like deep breathing in establishing consistent authentication patterns, irrespective of an individual's mental or physical state, including stress-induced conditions [22]. This underscores the necessity for authentication methods resilient to fluctuations across diverse mental and physiological states, ensuring reliability and consistency in practical applications [22].

In the study [16] that uses Emotiv EPOC+ headset, the focus lies on utilizing Event-Related Potentials (ERPs) as unique patterns of brainwave activity for authentication. The study underscores the advantages of brainwaves as biometrics, highlighting their resistance to external observability, revocability, and intrinsic liveness detection. The research delves into various experiments and protocols, such as P300 and N400 paradigms, to evoke specific brainwave responses. It outlines the acquisition, preprocessing, feature extraction, and classification processes involved in authentication. Usability considerations and security concerns, alongside challenges in comparability and consistent performance metrics, are also addressed.

[17] explores EEG-based authentication systems, emphasizing the individualistic nature of EEG signals and their potential in enhancing security and convenience. The study involves recruiting healthy adult participants, recording EEG data, and performing classification using Auto-WEKA. Results indicate the system's accuracy in distinguishing user-specific instances and evaluating metrics such as False Acceptance Rate (FAR), False Rejection Rate (FRR), and Area Under the Receiver Operating Characteristic curve (AUC). The system description outlines the user registration process and database management for authentication.
The research aims to utilize event-related potential (ERP) for authentication purposes, leveraging audio and visual stimuli. ERP, as explained [20], refers to the brain's electrical activity captured through EEG signals in response to specific stimuli or events. These events can be external stimuli or the actions and responses of the individual being studied. [21] highlights that while simple tasks like resting states are prone to environmental noise and artifacts, tasks involving mental activities or responses to external stimuli provide clearer signals, known as a higher "signal-to-noise ratio" (SNR). ERP analysis enhances this clarity, offering researchers a precise and reliable method to isolate and analyze specific brain responses. This approach is particularly appealing for authentication purposes due to ERP's higher signal-to-noise ratio, as noted [16]. Thus, the study seeks to capitalize on ERP's effectiveness in isolating and analyzing brain responses for authentication.

B. Objectives of the Study

The general purpose of this study is to develop and present a brainwave authentication system as a way to utilize biometrics. The authentication system will not only serve as an innovation but enhances current security measures available. Through in-depth study of its implications, vulnerabilities, and applicability this study would like to improve the biometric technologies.

To accomplish the mentioned objectives, it will be split into specific objectives that align with the development and utilization of the application:

1. To identify the unique brainwave patterns that can be reliably used for user authentication

2. To develop and implement a brainwave authentication system that can capture, analyze, and authenticate registered users

3. To be able to authenticate users with their brainwave and reject invalid users

4. To evaluate the performance and accuracy of the brainwave authentication system using False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (ERR) as the metrics.

C. Significance of the Study

This study will be conducted to examine the significance of introducing a brainwave authentication system as a new process of biometrics. The approach of this proposed research can improve user identification and safety of their credentials.

Benefiting the study are the various sectors as follows:
Users. Help users by introducing a new login method that will secure their information and valuable biometric authentication.

Software Developers. The developed system will help developers design and implement a secure and user-friendly brainwave authentication system.

Security Experts and Analysts. One of the main focus of the study is to share findings and insights of a brainwave authentication system to security analysts which will help them understand a new way of biometric system in the country.

Future Researchers. The result of this study can serve as a foundation for future studies that will be conducted for a brainwave authentication system or similar system.

D. Scope and Limitations

The study covers the development of a brainwave authentication system that will capture, analyze, and authenticate registered users through electroencephalography (EEG) readings of users' brainwave. The algorithm will aim to identify unique patterns in brainwave signals for individual users.

The EEG recording was collected using a 64 channel Easycap device with sampling rate of 1000 Hz and downsampled to 250 Hz in the segmented epochs available in the dataset. The dataset that is collected by the researcher, M3CV database contains 14 types of EEG tasks from 106 healthy young adults (73 male & 33 female). 95 participants with an average age of 21.3 years old completed two experimental sessions on different days. The two sessions are separated within the range of 6 days to 139 days for each participant with an average between session time of 20 days.

Participants included in study have normal hearing, normal or corrected vision, and no neurological condition. For the well-being of the participants, they are asked to sit in a chair and one-meter away from the screen if a visual input is needed. The experiment lasts for 2 hours (total of 50 mins for recording and total of 70 minutes for resting between each run). Five experts in neuroscience ensure data quality for each task. In this study focusing on event-related potential, the researchers will utilize the task on the paradigm of Transient-state sensory stimuli on audio, visual, and touch with each having 60 trials.

Transient-state sensory stimuli lasted 50 milliseconds. The dataset that are collected are clean and segmented by the dataset provider with each file containing 1-4 second of EEG recording per user. In addition, this study will only utilize 3 tasks out of 14 tasks available in the dataset. Those tasks are task 3 (visual stimuli task), task 4 (auditory stimuli task), and task 5 (touch stimuli task).

The scope of the study includes preprocessing of EEG data, feature extraction using Convolutional Neural, and application of Support Vector Machine for classification. For feature extraction, all frequency bands such as alpha, beta, theta and delta will be extracted. In addition, the performance of the classification model is subject to the quality and diversity of the training data. The study will evaluate the authentication's accuracy through False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER).

The dataset utilized in this research is publicly available and sourced from Kaggle. As this dataset was not collected by the researchers, relying on the data's completeness, accuracy, and quality are on the original dataset contributors. The generalizability of our findings will be constrained by the features and characteristics of the M3CV conducted by the dataset provider. In addition, factors that might limit the study, such as data collection methods, participants diversity, and recording conditions are beyond the control of this study.

E. Conceptual Framework

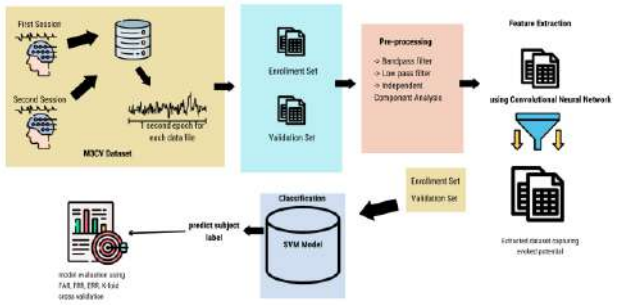

Figure 1.1. Conceptual Framework of the Study

F. Operational Definition of Terms

Area under the curve - metric used to evaluate the performance of classification models.
Authentication - confirming the identity of a user through credential or biometric information, to gain access to a secured service.
Auto-WEKA - machine learning tool that automates the selection and tuning of classification algorithm.
Biometrics - method of authentication that relies on unique physical or behavioral characteristics of individuals such as fingerprints or in this study brainwave patterns to verify identity.
Brainwave authentication - authentication method that utilizes electroencephalography (EEG) to analyze and authentication individuals based on unique patterns of their brainwave activity.
Classification - assigning predefined labels to input data based on learned patterns or features.
Electroencephalography - technique for recording electrical activity in the brain through electrodes placed on the scalp, commonly used in medical and research settings to study brain activity.
Event-related potential - measured brain response resulting from a specific event or stimuli (e.g., an image recognized by the user) captured through electroencephalography (EEG) and used in an authentication system to identify unique brainwave patterns.
False acceptance rate - rate at which unauthorized users are incorrectly accepted by the authentication system as genuine, indicating the system's vulnerability to impostors.
False rejection rate - rate at which legitimate users are incorrectly rejected by the authentication system, indicating the system's tendency to deny access to authorized users.
Feature extraction - process of identifying and selecting relevant information from raw data to create representation for analysis or classification.
High signal-to-noise ratio - measure of the strength of a desired signal relative to background noise, indicating the clarity and reliability of the signal captured by a recording or measurement device.
Two-factor authentication - security process that requires users to provide two different authentications (e.g., password and fingerprint scan) to verify their identity.
Verification - act of confirming the authenticity of a claimed user through comparison of stored reference of a user.

G. Table of Abbreviations

2FA	Two-Factor Authentication
AEP	Auditory Evoked Potential
AUC	Area Under the Curve
AUTO-WEKA	Automated-Waikato Environment for Knowledge Analysis
DNA	Deoxyribonucleic Acid
DWT	Discrete Wavelet Transform
EEG	Electroencephalography
EER	Equal Error Rate
ERP	Event-Related Potential
FAR	False Acceptance Rate
FIR	Finite Impulse Response
FRR	False Rejection Rate
N400	Negative 400
P300	Positive 300
SDK	Software Development Kit
SEP	Somatosensory Evoked Potential

SNR	Signal-to-Noise Ratio
SVM	Support Vector Machine
VEP	Visual Evoked Potential

CHAPTER II

Review of Related Literature

A. Biometric Authentication Methods

Overview of traditional techniques (passwords, 2FA)

Authentication methods have evolved significantly over the years, with traditional techniques like passwords and two-factor authentication (2FA) being widely adopted. Passwords, the most basic form of authentication, rely on something the user knows. Despite their simplicity, passwords have inherent vulnerabilities such as susceptibility to brute-force attacks, phishing, and poor password hygiene among users [25]. Two-factor authentication (2FA) was introduced to add an additional layer of security. It combines something the user knows (password) with something the user has (like a mobile device for receiving a verification code), thus providing a higher level of security compared to passwords alone [2].

Despite the enhanced security provided by 2FA, it is not foolproof. Methods such as SIM swapping and sophisticated phishing attacks can still compromise 2FA systems [7]. Multi-factor authentication (MFA) further enhances security by incorporating additional verification steps, such as biometric data, thus making unauthorized access significantly more difficult [7].

Advances in biometric technologies (fingerprint, facial recognition, EEG)

Biometric technologies have advanced considerably, providing more secure and user-friendly authentication methods. Fingerprint recognition, one of the earliest biometric technologies, has become ubiquitous in smartphones and access control systems due to its reliability and ease of use [3]. Facial recognition has gained popularity for its non-intrusive nature and ability to authenticate users seamlessly without physical contact [4].

Electroencephalography (EEG), which captures brainwave activity, represents a newer frontier in biometric authentication. EEG-based authentication leverages the uniqueness of brainwave patterns to identify individuals, offering advantages in security and privacy [5]. Unlike other biometric methods, EEG signals are difficult to replicate or steal, making them a promising solution for high-security applications [5].

B. EEG Brainwave Authentication

Introduction and advantages of using EEG for authentication

EEG brainwave authentication is a cutting-edge biometric method that leverages the unique electrical activity patterns of an individual's brain. This method offers several advantages over traditional and other biometric systems. For one, brainwave patterns are highly individualized and difficult to duplicate, providing a robust form of security [5]. Moreover, EEG-based authentication can be performed continuously, offering real-time verification without requiring user intervention [5].

Using EEG for authentication can also enhance user convenience. Unlike passwords or physical tokens, which can be forgotten or lost, brainwave patterns are intrinsic to the user, eliminating the need for users to remember complex passwords or carry additional devices [10][14]. Additionally, EEG signals are less susceptible to environmental factors that might affect other biometric methods, such as lighting conditions in facial recognition systems [11][18].

Technical aspects of EEG signal acquisition

Acquiring EEG signals for authentication involves placing electrodes on the user's scalp to detect electrical activity generated by the brain. This requires precise placement and high-quality sensors to ensure accurate signal capture [9]. The captured signals are typically very weak and require amplification and filtering to be useful for pattern recognition [20].

The pattern recognition process in EEG-based authentication systems involves several steps. First, the raw EEG data undergoes preprocessing to remove noise and artifacts. This step is crucial as EEG signals are often contaminated by muscle activity, eye movements, and external electrical interference [21]. After preprocessing, feature extraction is performed to identify relevant characteristics of the EEG signals, such as frequency bands and amplitude [20]. Machine learning algorithms, like Support Vector Machines (SVM) and Artificial Neural Networks (ANN), are then employed to classify and recognize the patterns specific to each individual [15].

Pattern recognition in EEG signals

Pattern recognition in EEG-based authentication systems is a complex process that involves several stages of signal processing and analysis. The first stage is signal preprocessing, which includes techniques such as band-pass filtering to isolate specific frequency ranges and artifact removal to eliminate noise from muscle movements and external sources [21]. Following preprocessing, feature extraction methods such as Fast

Fourier Transform (FFT) and wavelet transform are applied to identify distinguishing characteristics of the EEG signals [20].

Machine learning algorithms play a crucial role in the pattern recognition process. Support Vector Machines (SVM) and Artificial Neural Networks (ANN) are commonly used for their ability to handle high-dimensional data and classify complex patterns [15]. These algorithms are trained on labeled EEG data to learn the unique brainwave patterns of each individual. During authentication, the system compares the real-time EEG data with the stored patterns to verify the user's identity [13].

The integration of EEG-based authentication into practical applications poses challenges, such as the need for user-friendly and non-intrusive EEG acquisition devices. Advances in wearable technology are addressing these challenges by developing compact and comfortable EEG sensors that can be easily integrated into everyday devices [9]. The combination of advanced signal processing techniques and powerful machine learning algorithms makes EEG-based authentication a promising solution for secure and reliable user identification [5].

Local Research about EEG System

Research on brainwave authentication systems in the Philippines is currently limited. Most EEG-related studies in the country focus on different applications. For example, the study by [27] titled "Exploring the Relationship Between EEG Features of Basic and Academic Emotions" investigates how EEG can be used to understand emotional responses in academic settings. This research was conducted to explore the EEG features correlated with various emotional states during learning activities.

Another study [26] titled "Development, Evaluation, and Analysis of Biometric-Based Bank Vault User Authentication System Through Brainwaves" is one of the few exploring EEG in authentication. This study aimed to develop and evaluate a brainwave-based user authentication system for bank vaults. It involved collecting EEG data from participants and using machine learning algorithms to authenticate users based on their brainwave patterns.

Overall, while foundational research on EEG exists in the Philippines, studies specifically targeting brainwave authentication systems remain sparse, highlighting the need for further exploration in this promising field.

Addressing variability and external influences on EEG patterns

One of the primary challenges in EEG-based authentication systems is the variability in EEG patterns caused by both intrinsic and extrinsic factors. Intrinsic factors include individual differences in brain anatomy and physiology, which can lead to variability in brainwave signals even among healthy subjects [10][14]. Extrinsic factors, such as environmental noise, physical state (e.g., fatigue, stress), and electrode placement, can also significantly affect the quality and consistency of EEG signals [28].

Addressing these variabilities requires robust preprocessing and signal enhancement techniques. Noise reduction methods, such as artifact removal algorithms, are essential to filter out unwanted signals caused by muscle movements or external electrical sources [21]. Furthermore, normalization techniques can help standardize EEG data across different recording sessions, thereby improving the reliability of the authentication process [20].

Adaptive machine learning algorithms that can learn and adjust to individual variability over time are also crucial. These algorithms can incorporate user-specific calibration sessions to account for personal differences and improve classification accuracy [13]. Continuous learning models that update and refine themselves with new data can enhance the system's ability to handle day-to-day variations in EEG patterns [15].

Potential enhancements and future applications in cybersecurity

The future of EEG-based authentication lies in enhancing the technology to make it more practical and user-friendly. One potential enhancement is the development of more advanced and less intrusive EEG acquisition devices. Wearable EEG sensors integrated into everyday accessories like glasses or headbands could make the technology more accessible and convenient for regular use [9]. These advancements will not only improve user compliance but also the quality of the EEG signals collected.

Another promising direction is the integration of EEG-based authentication with other biometric methods to create multi-modal biometric systems. Combining EEG with fingerprints, facial recognition, or voice recognition can significantly enhance the overall security by leveraging the strengths of each method while compensating for their weaknesses [2]. Such multi-modal systems can provide higher accuracy and robustness against spoofing attacks compared to single-modality systems [3].

In terms of applications, EEG-based authentication has significant potential in the field of cybersecurity. It can be used to protect sensitive information and critical systems by ensuring that only authorized users can gain access. This is particularly relevant for high-security environments such as government facilities, financial institutions, and military operations [5][8]. Furthermore, continuous authentication systems that monitor user identity in real-time can prevent unauthorized access even if the initial login was compromised [4].

Research is also exploring the use of EEG-based authentication in emerging technologies like brain-computer interfaces (BCIs). BCIs, which allow direct communication between the brain and external devices, can benefit from secure and reliable authentication methods to prevent unauthorized use and ensure user privacy [15]. As BCI technology advances, integrating EEG-based authentication could become a standard feature, enhancing the security of these innovative systems.

Stability and Reliability of EEG Authentication System

In their 2018 study, [1] explore the application of advanced signal processing techniques to enhance the robustness of EEG systems. One of the key methods they focus on is Common Spatial Patterns (CSP). The CSP approach is a classical and representative technique in the brain-computer interface (BCI) community, used for optimizing spatial filters of EEG signals. It maximizes the variance difference between two classes of signals, facilitating better distinction between different mental states [29]. However, CSP primarily utilizes only the amplitude information of the EEG signals. Despite this limitation, it effectively isolates brain signal features that are less susceptible to transient internal states, thereby improving the reliability of BCIs.

Another significant technique is Independent Component Analysis (ICA). ICA is a computational method for separating the original signals from the interfered signals. It decomposes interfered signals into non-Gaussian signals and is a mathematical method for discovering hidden signals. ICA defines a generative model for the observed multivariate data, which is typically given as a large database of samples. In this model, the data variables are assumed to be linear mixtures of some unknown latent variables, and the mixing system is also unknown. By separating EEG signals into statistically independent components, ICA aids in the isolation of neural sources from artifacts. This separation is crucial for enhancing the clarity and accuracy of EEG signals, as it allows for the removal of noise and other non-neural interferences. By incorporating ICA, the study demonstrates significant improvements in the performance and robustness of EEG-based systems [30].

The study by [1] underscores the potential of these advanced signal processing methods in addressing the challenges posed by variability in brain signals. By employing CSP and ICA, researchers can develop more accurate and reliable BCIs, paving the way for more effective applications in various fields such as neurorehabilitation, communication, and control. This review highlights the importance of enhanced signal processing techniques in the ongoing development of robust and efficient EEG systems.

Regular calibration

Regular calibration procedures are essential for maintaining the long-term reliability and effectiveness of EEG authentication systems. By implementing a systematic recalibration process, these systems can adapt to changes in users' brainwave patterns caused by factors such as aging or health fluctuations. According to a study [31], regular recalibration significantly enhances the reliability of EEG-based biometric systems by ensuring that they remain aligned with the evolving characteristics of users' brain signals. This adjustment mechanism mitigates

the risk of performance degradation over time, thereby sustaining the accuracy and robustness of the authentication process. Incorporating regular calibration procedures alongside advanced signal processing techniques provides a comprehensive approach to optimizing the performance of EEG authentication systems in real-world scenarios.

Justification

EEG signals, with their intricate reflection of the brain's neural activities, offer inherent security owing to their uniqueness and difficulty in replication or forgery. This quality positions EEG as a prime candidate for applications where security is paramount. [32] underscored the potential of EEG in secure environments, highlighting its resilience against forgery due to the personalized and complex nature of brainwave patterns. Their research emphasizes the robustness of EEG-based authentication systems, which leverage the distinct characteristics of individual brain signals to establish reliable and secure identification protocols. By harnessing the distinctive features of EEG signals, such systems provide a robust defense against unauthorized access and impersonation attempts, making them invaluable for safeguarding sensitive information and ensuring secure interactions in various domains.

Moreover, EEG-based authentication systems offer a non-intrusive and user-friendly approach to identity verification, making them suitable for a wide range of applications, including healthcare, finance, and technology. Unlike traditional authentication methods that often rely on passwords or biometric data susceptible to theft or replication, EEG-based systems offer a unique advantage by directly tapping into the user's neural activity. This approach not only enhances security but also ensures convenience and ease of use for individuals across diverse demographics. As demonstrated by [32] , EEG-based authentication systems can seamlessly integrate into existing security frameworks, providing a reliable and efficient means of identity verification without imposing additional burdens on users.

Furthermore, the adaptability of EEG-based authentication systems makes them well-suited for dynamic environments where user characteristics may change over time. With regular calibration procedures, these systems can adjust to long-term changes in users' brainwave patterns, ensuring consistent and accurate authentication performance. This adaptability is particularly crucial in scenarios where users' health conditions, aging processes, or other factors may influence their EEG signals. By implementing regular calibration protocols, organizations can enhance the long-term reliability of EEG-based authentication systems, mitigating the impact of variability in users' brain activity and maintaining robust security standards over time. Additionally, EEG signals are not exposed to intruders, making them uncapturable and thus, difficult to forge [33]. This inherent property adds another layer of security to EEG-based authentication systems, further fortifying their resilience against fraudulent activities and unauthorized access attempts.

Dynamic authentication capabilities

Dynamic authentication capabilities provided by EEG offer a significant advantage over static biometric systems, enabling continuous authentication throughout user sessions. Unlike traditional methods that authenticate users only at the point of entry, EEG-based systems can monitor the user's identity continuously, ensuring ongoing security. [34] highlights this dynamic capability in his research on EEG as a biometric for continuous authentication systems. By leveraging EEG signals, these systems not only verify the user's identity during initial login but also maintain vigilance throughout the session, detecting any unauthorized access attempts or identity breaches in real time. This continuous monitoring enhances security by providing a robust defense against impersonation attacks and unauthorized activities, effectively safeguarding sensitive information and resources. Moreover, EEG-based authentication offers a seamless and user-friendly experience, eliminating the need for repeated authentication prompts and minimizing disruptions during user interactions. This capability makes EEG an invaluable tool for securing access to critical systems and resources in diverse domains, ranging from healthcare and finance to technology and beyond [34].

Adaptation to Different User Groups

To achieve consistent performance among varied users, brain-computer interface (BCI) systems must be tailored to different user groups through personalized calibration and rigorous feature selection. Personalized calibration is required because EEG signals are largely user-specific, impacted by genetic variances, brain shape, and personal experience. This includes an initial calibration phase in which each user's EEG data is collected to create a baseline profile matched to their own neurological tendencies. BCI systems can improve their accuracy and reliability in interpreting brain activity by addressing individual variances via tailored calibration [35]. This stage is critical to ensuring that the system can properly convert each user's unique brainwave patterns into accurate commands, hence improving user experience and system performance.

Robust feature selection is another critical aspect that enhances the adaptability and reliability of BCI systems across different user groups. The procedure entails identifying features from EEG data that are less vulnerable to external influences or subtle neurological changes. By focusing on invariant and discriminative features, the system may maintain consistent performance despite the inherent variability of EEG signals. This method not only enhances the accuracy of EEG pattern detection, but it also assures that the system remains functional over time and across sessions [1]. Implementing robust feature selection in conjunction with individualized calibration strengthens BCI systems' resilience to the dynamic nature of EEG signals, resulting in a more stable and dependable interface for users with diverse neurological profiles.

Introduction to Transient-State Sensory Stimulation

Sensory signals, such as Visual Evoked Potentials (VEP), Auditory Evoked Potentials (AEP), and Somatosensory Evoked Potentials (SEP), are transient-state signals that represent neural responses to sensory stimuli [36] [40]. Transient-state sensory stimulation refers to the elicitation of electrical potentials in the brain through brief, controlled stimuli in visual, auditory, and somatosensory modalities. These potentials, known as evoked potentials (EPs), provide insights into sensory processing and neural pathway integrity.

Offline assessments and simulation of online tests have enabled researchers to explore the complexities of these transient state sensory signals and identify difficulties and knowledge essential for the development of EEG-based biometric systems [41]. For instance, studies conducted regarding VEP have shown that there is a reduction in the level of accuracy as the population sizes increase, indicating scalability issues in VEP-based biometric systems [42]. Research on AEP has revealed the necessity of sound cross-session testing approaches to account for performance decline across recording sessions, underlining the need for valid and transportable AEP-based identification and verification systems [40]. Furthermore, research on SEP has highlighted issues such as reduced accuracy with increasing population size and the requirement for thorough cross-session testing methods for SEP-based biometric systems [42].

All these findings point to the fact that transient-state sensory signals in EEG-based biometrics are not straightforward, stressing the need for proper assessment paradigms to determine the reliability, scalability, and generalizability of the proposed methods under various conditions [41] [40]. As EEG-based biometric technology further develops, it will be important to address issues related to transient-state sensory signals to design and implement practical, efficient, and accurate biometric identification and verification systems. Moreover, enhancing the study of these transient-state sensory signals may help in understanding inter- and intra-subject variability and the signal processing and decoding methodologies in EEG [42].

Visual Evoked Potentials (VEP)

VEPs are initiated by brief visual stimuli and recorded from the scalp overlying the visual cortex. These potentials are crucial for assessing the functional integrity of the visual pathways. VEP waveforms are extracted from the electroencephalogram (EEG) by signal averaging, which enhances the signal-to-noise ratio by reducing the impact of unrelated background activity [37].

VEP is an integral part of EEG-based biometrics, which illustrates the brain's response to the visual stimuli [40]. To understand the dynamics of VEP performance, the study carried out extensive offline assessments and pseudo online examinations [41]. Interestingly, the study showed a significant decline in the accuracy of the VEP biometric system as the population sizes grew, thus indicating limitations in scalability. Furthermore, the study pointed out the need for reliable cross-session testing paradigms, which would guarantee the validity and transferability of VEP-based identification and verification procedures [42].

Auditory Evoked Potentials (AEP)

AEPs assess specific areas of the brainstem, midbrain, and auditory cortices. These potentials are elicited by acoustic stimuli, such as clicks, which trigger neural responses that travel from the auditory nerve to the cerebral cortex. AEPs are recorded using electrodes placed at the vertex and ear lobe. The extraction of AEPs from the background EEG and electromyogram (EMG) activity is achieved through signal-averaging techniques. AEPs are particularly valuable for monitoring patients during cardiovascular surgery due to their objectivity and reproducibility [39].

The analysis of AEP brings useful information concerning EEG-based biometrics, describing the neural response to auditory stimulus [40]. Through varied offline assessments and realistic online sample exams, the study explicated the dynamics of AEP performance across various scenarios [41]. Some of the important findings which were highlighted include the fact that accuracy decreases over recording sessions, which calls for the need to have proper ways of testing cross sessions so as to be in a position to address issues of degradation [42]. Furthermore, the study established that it was difficult to develop AEP-based biometric systems that could be resistant to changes in mental state, underlining the need for proper assessment frameworks [40].

Somatosensory Evoked Potentials (SEP)

SEPs are electrical signals generated by the nervous system in response to somatosensory stimuli. These potentials can be recorded at various levels of the somatosensory pathway, including the scalp and cervical spine. SEPs are typically elicited by transcutaneous electrical nerve stimuli of 0.2–2-ms duration, applied to the median and posterior tibial nerves. The latency and amplitude of SEPs are analyzed to identify and monitor impairments in the somatosensory pathways [38]. SEPs are used clinically to diagnose and monitor conditions affecting the peripheral and central nervous systems, such as spinal cord injuries and multiple sclerosis.

EP are widely used in EEG-based biometrics as they represent neural responses to somatosensory stimuli [40]. To determine SEP performance under different circumstances, the study used offline assessments and simulated online quizzes [41]. Some of the findings highlighted issues like decline in accuracy as the population size increases, thus highlighting the need for scalable SEP-based biometric systems [42]. Moreover, the research pointed out the issue of stability and preservation across the recording sessions and underlined the necessity to develop reliable cross-session testing methods to increase the stability of the results [40].

CHAPTER III

Methodology

A. Participants and Apparatus

Participants

The study involved 106 healthy volunteers from Shenzhen University. 95 of them (average age 21.3 years, mostly male) participated in two separate sessions, spaced between 6 to 139 days apart (average 20 days). Everyone had normal hearing and vision (with or without corrections) and no history of neurological problems or disorder. They sat comfortably about a meter from a screen during the experiment.

To highlight, this research will only utilize participant 1 - 85 as data point and the registered users where their EEG recordings will be utilized for training the model acting. On the other hand, three participants outside of participant 1-85 will act as intruder users where they will not be a part of training data and will try to be accepted by the model and the model's goal is to reject them consistently.

The university's ethics committee approved the research. All volunteers were informed about the experiment beforehand and signed consent forms allowing their anonymized data to be used for future research.

Furthermore, the dataset that will be used in this study are validated locally by Dr. Joshua Mark P. Nombre, M.D. In the certification, Dr. Nombre stated that the dataset is fully validated and in line with normal human EEG findings. In addition, the EEG recordings are all legitimate and proved to be real electroencephalography readings.

Apparatus

The study used an EEG amplifier BrainAmp to record brain activity (EEG signals) while people were shown or heard different things (stimuli). The brain activity was recorded using an Easycap EEG device at a sampling rate of 1000Hz by 64 electrodes.

For sight-related tasks (VEP and SSVEP), a bright light was used. For hearing tasks (AEP and SSAEP), a headphone delivered a specific sound. For touch tasks (SEP and SSSEP), a small vibration motor was used. For some tasks, a computer screen was used to show pictures or instructions. A special program which is Psychtoolbox helped create these images.

Figure 3.1. 64 channel Easycap device for EEG recording

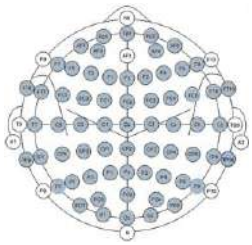

Figure 3.2. Easycap electrode map

B. EEG Dataset Acquisition

Dataset Acquisition

The study will utilize an open access database of Gan H., Zhen L., & Zhiguo Z. (2022) [47] that is found on Kaggle. The dataset was utilized by the researchers in the goal of adding contribution to existing M3CVs (Multi-subject, Multi-session, and Multi-task Database for Investigation of EEG Commonality and Variability) which is large-scale database in researching EEG signals across different subjects, sessions, and tasks.

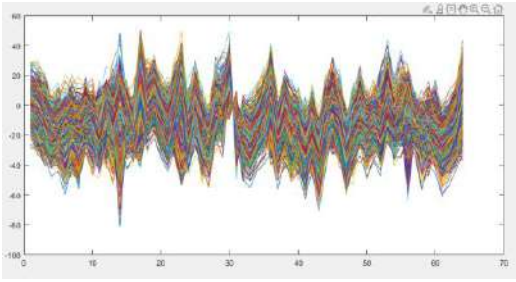

Figure 3.3. Example of plotted epoch data file

Dataset Composition

The dataset was separated into three categories: Enrollment, Calibration, and Testing each serves a distinct purpose in the development of an EEG-based authentication system. The collection of EEG reading to the participant was done in two sessions on two different days. Enrollment phase was collected on the first session from 95 participants. Creating and establishing EEG profiles for every participant is important as the basis for the biometric system. Calibration phase was collected from the second session from 20 subjects in the goal of fine-tuning the machine learning model that will be used in the system. Testing phase was also collected from the second session composed of 86 subjects which includes 11 intruders in the goal of adding variability in the dataset.

In this research due to the limitation of the testing folder and the dataset itself, the testing folder lacks correct labels provided by the dataset source. As a result, the researcher will allocate 20% of enrollment folder and calibration

folder for evaluating the model's performance on unseen data of registered and intruder users and the remaining 80% will be used for training the model.

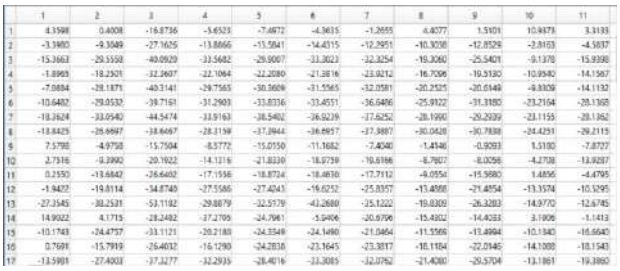

Figure 3.4. *Raw numerical value of a data file*

The dataset column header represents the time in milliseconds (0-1000 ms) while the rows represent the EEG recording for each 64 channel of the device. Row 65 of the dataset represents the event marker where the stimulus or events happens (see Figure 3.5)

Experiment Design

On the M3CV dataset there are a total of fifteen tasks also stating the specific run in the session.

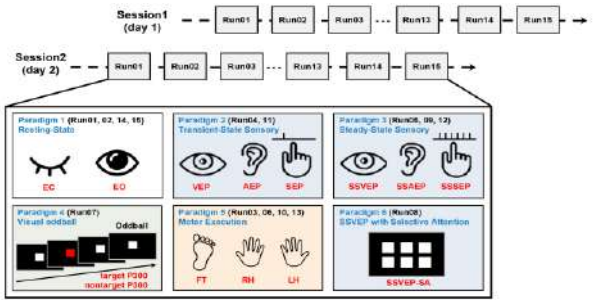

Figure 3.5. Dataset tasks and run

Table 3.1. Stimuli tasks and abbreviation

Task	Abbreviation
Eyes Closed	EC
Eyes Open	EO
Visual Evoked Potential	VEP
Auditory Evoked Potential	AEP
Somatosensory Evoked Potential	SEP
Steady-State Visual Evoked Potential	SSVEP
Steady-State Auditory Evoked Potential	SSAEP
Steady-State Somatosensory Evoked Potential	SSSEP
P300 (Target and Nontarget)	P300
Foot Motor Execution	FT
Right Hand Motor Execution	RH
Left Hand Motor Execution	LH
Steady-State Visual Evoked Potential with Selective Attention	SSVEP-SA

Figure 3.4 and Table 3.1 display the tasks defined in the gathered dataset which consist of thirteen tasks overall and 15 run across two sessions. This research study will utilize Task 3 VEP (in response to visual stimuli), Task 4 AEP (auditory stimuli), and Task 5 SEP (touch stimuli). The researchers chose these three specific tasks which are Transient-state sensory tasks as they represent neural response to sensory stimuli. These tasks are inclined with the research goal of utilizing event-related potential (ERP) that is a presentation of a quick stimulus or event and on this research the stimuli lasts for 50 milliseconds.

The dataset provided are already segmented into epochs. For the enrollment phase the researchers will only utilize VEP, AEP, and SEP which are Task 3, 4, and 5 respectively. In the enrollment phase 57,851 epochs are present, after removing unnecessary tasks only 12,180 epochs will be fed in the classification model.

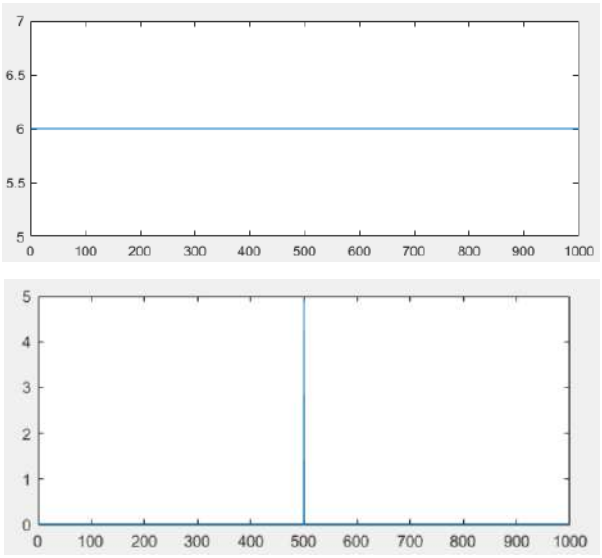

Figure 3.6. Steady-state sensory (Top) and Transient-state sensory (Bottom)

The researcher would like to utilize event-related potential and transient-state sensory fits the criteria of a one time stimuli compared to other tasks present in the dataset like in Figure 3.5 where the right figure represents steady-state sensory as a constant stimulus across EEG reading.

C. Preprocessing

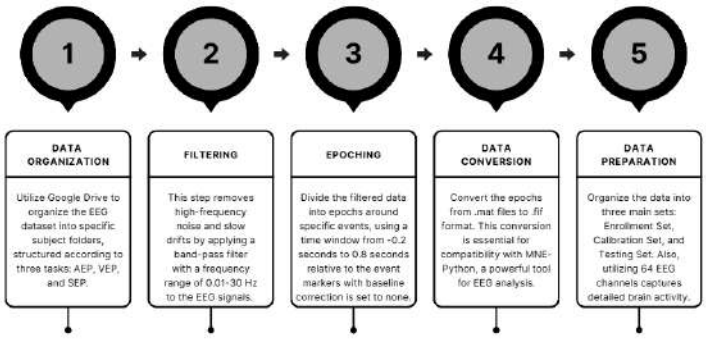

Figure 3.7. Workflow Steps for EEG Data Preprocessing

Pre-processing the dataset is important in obtaining EEG recording that will enhance the raw data before analysis. On the study of Gan et. al (2022), a band-pass filter of 0.01-200 Hz and notch filter of 50 Hz was used. Band-pass filter will allow signals within 0.01 Hz to 200 Hz to pass through, discarding and ignoring signals outside of that range. 0.01 Hz will help in removing slow drifts while 200 Hz will remove high-frequency noise that is included in the recording. Moreover, a notch filter was used to remove specific frequency in the recording. 50 hz was removed as it is commonly an interference caused by electrical mains of frequency that can introduce unwanted noise. Utilize Independent Component Analysis (ICA) in separating electrical signals specifically eye blinks and eye movements in the recorded EEG.

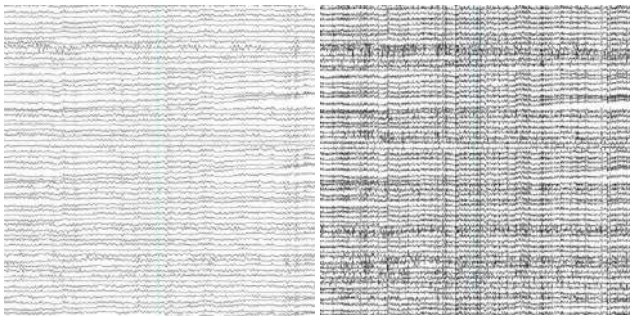

Figure 3.8. Raw and Filtered Data

To ensure proper organization and efficient processing, we utilized Google Drive to host the dataset, comprising EEG data from 95 subjects (sub001-095) across three specific tasks: Auditory Evoked Potentials (AEP), Visual Evoked Potentials (VEP), and Somatosensory Evoked Potentials (SEP). These tasks were chosen due to their relevance in capturing distinct brainwave patterns that are crucial for authentication systems. By organizing the data this way, we aimed to facilitate systematic analysis and task-specific feature extraction. This structure allows for easier management of large datasets, enhances collaboration, and ensures that critical data processing steps can be consistently applied across all subjects.

To process the EEG data, we applied a 0.01-30 Hz band-pass filter. This helps keep the important brainwave signals while removing noise and very slow drifts. After filtering, we divided the data into smaller segments, or epochs, around each event. We set the time window from -0.2 seconds before the event to 0.8 seconds after, which is commonly used in similar research studies to capture brain activity before and after a stimulus. We didn't use any baseline correction, as we didn't need to compare the signal to a baseline. This approach ensures that the data is clean and ready for further analysis using our CNN and SVM models.

We worked with three primary datasets, each provided in zip files containing all the epochs: the Enrollment Set, Calibration Set, and Testing Set. The Enrollment Set is used for training the biometric model, allowing the system to learn the unique EEG patterns of each participant. The Calibration Set serves to analyze EEG data, identifying commonalities and differences across subjects, sessions, and paradigms. Finally, the Testing Set is used to evaluate the system's accuracy. While the original data was

provided in .mat format, we converted all the files into .fif format because it is widely used in EEG research for its flexibility, better compatibility with EEG analysis tools like MNE-Python. We utilized MNE-Python for this research due to its powerful capabilities in EEG, as well as its extensive support for preprocessing, epoching, and visualizing EEG data. Additionally, we are using 64 channels of EEG signals to ensure a high-resolution capture of the brain activity across the scalp, which will provide more detailed data for the biometric model.

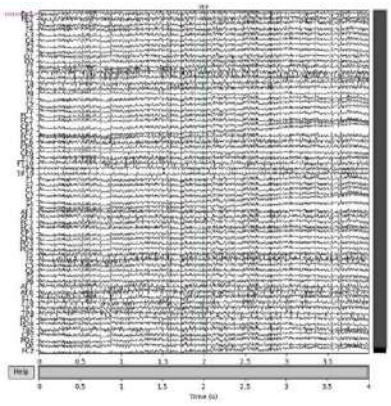

Figure 3.9. VEP response recorded across 64 EEG channels, demonstrating brain activity over a 4-second window.

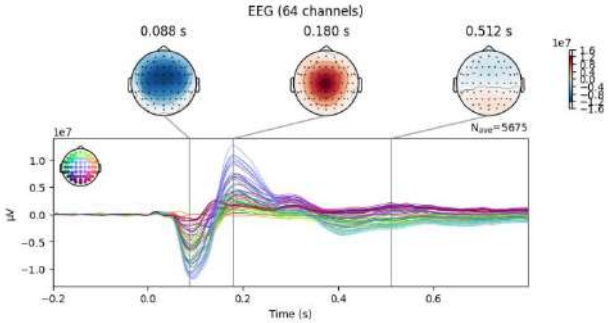

Figure 3.10. Evoked AEP from 64 EEG channels, averaged over 5675 trials, showing topographic brain activity at key time points post-stimulus.

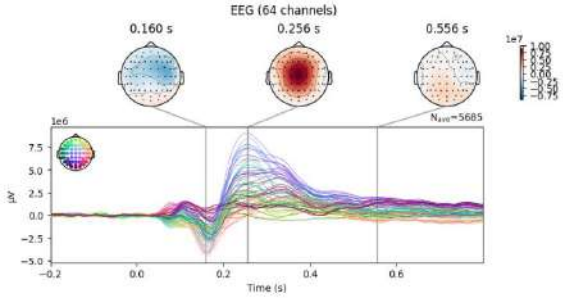

Figure 3.11. Evoked SEP from 64 EEG channels, averaged over 5685 trials, showing topographic brain activity at key time points post-stimulus.

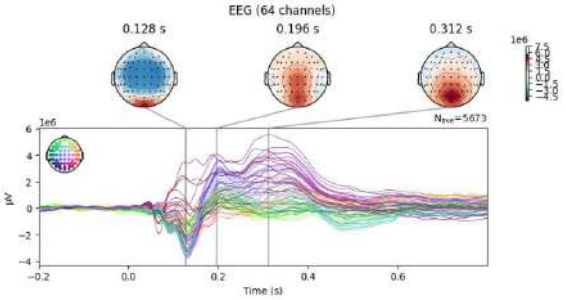

Figure 3.12. Evoked VEP from 64 EEG channels, averaged over 5673 trials, showing topographic brain activity at key time points post-stimulus.

D. Labelling

We used three main datasets in our research: Enrollment, Calibration, and Test datasets, corresponding to the VEP, AEP, and SEP tasks, respectively. The Enrollment dataset of Session 1 contained the 16,135 epoch files labeled for subject ID and then for task type. The epochs in the Calibration dataset of Session 2 were also labeled for the subject and task types. The Testing dataset was also from Session 2 with a total of 7,133 labeled epoch files. We classified the epoch files based on subject ID and particular tasks by using Python scripts in Google Colab. This approach leverages MNE-Python that has automated the process of EEG signal detection and the assignment of labels to it. Each task has a unique event marker-3 for VEP, 4 for AEP, and 5 for SEP. Interestingly, in the Testing dataset, subjects sub021 through sub090 are used with a usage of 4, which stands for verification and the unknown subject has a usage of 3 which stands for identification.

E. Feature Extraction

Convolutional Neural Networks (CNNs) are powerful deep learning models commonly used for image recognition, but their utility extends to extracting meaningful features from EEG signals. In the context of EEG-based authentication, CNNs are employed to automatically detect patterns in brainwave data that are difficult for manual feature extraction techniques to identify. CNNs are crucial for EEG feature extraction due to their ability to capture spatial features and relationships between neighboring electrodes through convolutional layers [51]. They facilitate hierarchical feature learning by using multiple layers of convolution and pooling. Moreover, CNNs efficiently reduce the dimensionality of EEG data without losing critical information, making them particularly effective for preprocessing large datasets in classification tasks. While CNN is known for its ability for image classification, over the years CNN has been utilized for analyzing EEG signals as well. In this research, CNN is used not for classification but for extracting unique features of the subject. [52] stated that EEG signals are unique and distinctive and through convolutional and hidden layers CNN can learn and extract unique features for every subject.

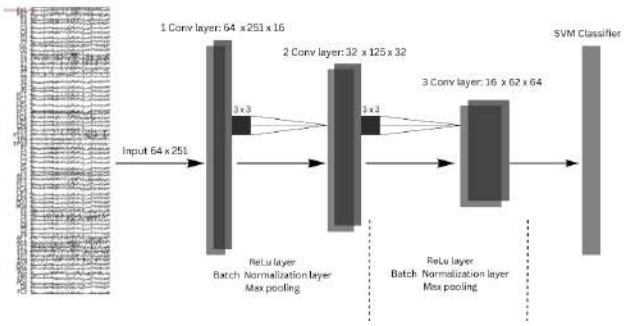

Figure 3.13. CNN-SVM Architecture

In our initial network topology (Figure 3.13), we employ a convolutional neural network (CNN) architecture consisting of three convolutional layers, each followed by a batch normalization layer to enhance stability and accelerate training. Additionally, we incorporate max pooling layers after each convolutional layer to down sample the feature maps, reducing dimensionality while preserving essential features.

- Input layer's input size is (64 x 251), representing 64 EEG channels, 251 time points.
- First Convolutional layer applies 8 filters of size (3 x 3) with kernel regularization to extract features from the input. Batch normalization ensures stable training, and max pooling (2 x 2) reduces spatial dimensions.
- The Second and Third convolutional layers employ 16 and 32 filters of size (3 x 3), respectively, utilizing ReLU activation to capture increasingly complex and high-level features from the data. Both layers incorporate batch normalization to stabilize activations and max pooling (2 x 2) to reduce spatial dimension, while the third layer also applies kernel regularization to enhance generalization and uses padding to maintain feature map size.
- The Flatten layer converts the multi-dimensional output from the previous convolutional and pooling layers into a one-dimensional vector. This transformation is essential for enabling the processed data to be fed into the subsequent dense layer.
- The Dense layer serves as the final output layer, consisting of 90 neurons that correspond to the possible output classes. By applying the 'softmax' activation function, it generates a probability distribution over these classes, allowing the model to predict the most likely class based on the features extracted from the convolutional layers.

The CNN-SVM Architecture as shown in (figure 3.13), employed a manual tuning of hyperparameters, requiring careful adjustments of filter sizes and configurations to identify the optimal settings for performance. This interactive process, while time-consuming, was crucial for fine-tuning the model's effectiveness in extracting relevant features from the EEG data. The insights gained from this initial phase informed the subsequent development of the revised model, which is illustrated in (figure 3.8).

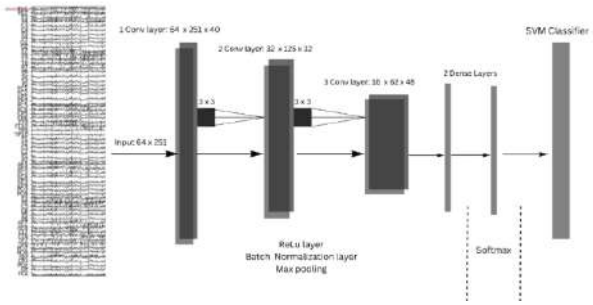

Figure 3.14. Revised CNN-SVM Architecture using Hyperband Tuner

In this revised network topology (figure 3.14), the key improvement over the initial model is the automation of hyperparameter tuning. Instead of manually setting hyperparameters such as the number of filters, kernel regularization values, dropout rates, dense units, and learning rates, this model defines these parameters within specific ranges. These ranges are automatically explored and optimized during the training process. By leveraging

this automated tuning, the revised model can efficiently identify the best configuration for each layer, significantly improving the model's performance and reducing the time spent on manual adjustments compared to the initial model.

- The First convolutional layer automatically selects the number of filters (between 8 and 64) and applies kernel regularization (values ranging from 0.001 to 0.1). Padding ensures the same output size, and max pooling reduces spatial dimensions.
- Like the First layer, the Second and Third convolutional layers automatically tune the number of filters (within the same range) and use ReLU activation. The third layer also applies kernel regularization. Batch normalization stabilizes training, and max pooling further reduces spatial size.
- The Flatten layer converts the 2D feature maps into a 1D vector, making it ready for classification.
- The Dense layer automatically tunes the number of dense units (between 8 and 128) with optional dropout for regularization, followed by a softmax layer for output classification.

After the features are extracted by the CNN, they are passed to the SVM for classification. The SVM uses these features to separate the data into distinct classes by finding the optimal decision boundary. This combination of CNN for feature extraction and SVM for classification leverages the strength of both methods, enhancing the overall accuracy of the model.

Layer (type)	Output Shape	Param #
conv2d_3 (Conv2D)	(None, 64, 251, 64)	640
batch_normalization_3 (BatchNormalization)	(None, 64, 251, 64)	256
max_pooling2d_3 (MaxPooling2D)	(None, 32, 125, 64)	0
conv2d_4 (Conv2D)	(None, 32, 125, 16)	9,232
batch_normalization_4 (BatchNormalization)	(None, 32, 125, 16)	64
max_pooling2d_4 (MaxPooling2D)	(None, 16, 62, 16)	0
conv2d_5 (Conv2D)	(None, 16, 62, 40)	5,800
batch_normalization_5 (BatchNormalization)	(None, 16, 62, 40)	160
max_pooling2d_5 (MaxPooling2D)	(None, 8, 31, 40)	0
flatten_1 (Flatten)	(None, 9920)	0
dense_2 (Dense)	(None, 104)	1,031,784
dropout_1 (Dropout)	(None, 104)	0
dense_3 (Dense)	(None, 90)	9,450

Figure 3.15. Revised CNN-SVM Architecture using Hyperband TunerSummary of CNN Model Architecture and Parameters

The total params represent the sum of all parameters in the model, including both trainable and non-trainable parameters. In this case, the model has 3,171,680 parameters in total. Out of these trainable params (1,057,146) are the parameters that the model learns and updates during training, such as weights and biases in layers like convolutional or dense layers. The non-trainable params (240) remain fixed and are not updated during training. Additionally, the optimizer params (2,114,294) refer to the extra parameters used by the optimizer, which helps in managing updates efficiently, such as storing values for momentum or learning rate adjustment.

F. Classification

Support Vector Machines (SVM) is supervised machine learning creating a decision boundary known as hyperplane. SVM will take advantage of support vectors which are data points that will separate groups. SVM will be utilized to classify EEG signal features into authentic users and potential intruders.

Support Vector Machine will be initially trained using the enrollment set, consisting of data collected from 95 participants. 17034 data will be fed in the classification model.

In refining the SVM model, the calibration set will be used. This consists of data from a subset of 20 participants during the second session. The dataset goal of having a calibration set is to fine-tune the model by using the additional data points and ensuring the machine learning model will adapt to any variability in EEG signals across different sessions (first and second session of collecting data). This will address and help in facilitating intra-subject and inter-session variability.

Testing set will be used to evaluate the performance of the SVM model. The testing set includes 86 subjects, which includes 11 intruders collected during the second session. The model will predict whether the EEG signals belong to authentic users.

Hyperplane - SVM goal is to find the hyperplane that maximizes the margin between two classes. The margin is defined as the distance between the hyperplane and data points from each class known as support vectors. Larger margin means better generalization of the classifier.

Support Vectors - are elements of the training set that are closest to hyperplane. Support vectors which are data points directly influence the position of the hyperplane. By focusing on these critical points, SVM will handle high-dimensional data and avoid overfitting.

Kernel Trick - SVM will employ a kernel trick if the data is not linearly separable in its original feature space. It will

map the features into a higher dimensional space where a hyperplane can effectively separate the classes.

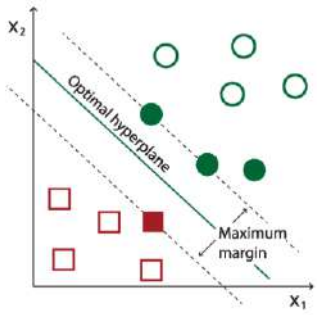

Figure 3.16. Support Vector Machine Visualization

Figure 3.16 displays the visualization of how a support vector machine works. The shaded green circle and red square shape represent the support vectors that are closest to the hyperplane that separate the class boundary. Support vectors create the hyperplane that maximize margin classification and minimize classification error.

G. Authentication System Evaluation

The model and its performance will be evaluated by False Acceptance Rate (FAR), False Rejection Rate (FRR), and Accuracy (ACC). FAR will assess how often imposter incorrectly authenticates as legitimate. FRR will indicate the frequency legitimate users are rejected, Accuracy will evaluate the proportion of correct predictions out of the total prediction made by the model.
Evaluation will also employ Equal Error Rate (EER) which finds the point where FAR and FRR are equal. The point will represent the points where the system has an equal chance of making a false acceptance and a false rejection [16].

$$FRR = \frac{FN}{FN + TP}$$

$$FAR = \frac{FP}{FP + TN}$$

$$EER = \frac{FAR + FRR}{2}$$

Figure 3.17. False Rejection Rate, False Acceptance Rate, and Equal Error Rate Formula

True Positive (TP) - occurs when the model correctly identifies a legitimate user as legitimate

False Positive (FP) - occurs when the system incorrectly identifies an intruder as legitimate user
True Negative (TN) - occurs when the system correctly identifies an intruder as not being the legitimate user
False Negative (FN) - occurs when the system incorrectly identifies a legitimate user an an intruder

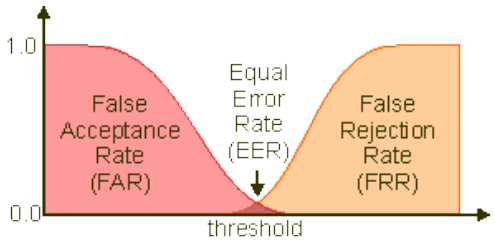

Figure 3.18. Equal Error Rate Visualization

Figure 3.18 shows the visualization of EER as a metric for evaluating the accuracy of the brainwave authentication system. The balance of FAR and FRR represents the threshold at which the system achieves balance between FP and FN. Lower EER indicates an acceptable performance signifying the system can distinguish legitimate users and intruders.

H. Development Environment

The research software setup was conducted entirely on Google Colab, a hosted Jupyter notebook that provides both CPU and GPU resources. Google Colab was selected for its convenience and reliable computing power, particularly useful during model training.

For EEG preprocessing and visualization, MNE-Python version 1.8.0 was used. The Convolutional Neural Network (CNN) Sequential model was built with TensorFlow version 2.17.0 and Keras version 3.4.1. Additionally, after constructing the model, Keras Tuner version 1.4.7 was used to fine-tune hyperparameters of the initial CNN model.

CHAPTER IV

Results and Discussion

4.1 Identifying Unique Brainwave Patterns for User Authentication

4.1.1 Preprocessing EEG Data

The first step in identifying unique brainwave patterns for authentication is extracting significant features from the raw EEG data. To process this, we used EEG signals recorded under specific tasks, including Auditory Evoked Potentials (AEP), Visual Evoked Potentials (VEP), and Somatosensory Evoked Potentials (SEP). Each of these tasks represents transient-state sensory stimuli that provoke distinct neural responses, making them ideal for identifying unique brainwave patterns. [48] ERP features are particularly discriminative because they reflect responses from specific neural circuits, making EEG a strong candidate for reliable biometric use. Furthermore, ERP's high-level processing of cognitive functions such as attention and memory provides valuable, individual-specific information that supports its accuracy and stability in biometric identification systems [49].

The raw EEG data was processed through band-pass and notch filters to remove artifacts and noise, ensuring that only relevant frequency bands (such as alpha, beta, delta, and theta) were included for analysis.

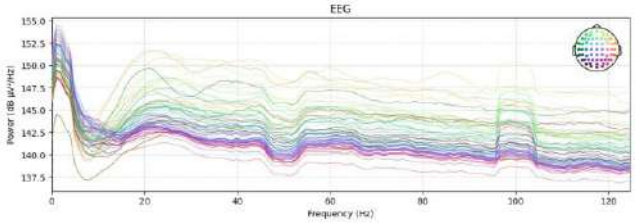

Figure 4.1. Power Spectral Density (PSD) for Unfiltered EEG Data

This figure presents the power spectral density of unfiltered EEG signals across multiple channels, with power (dB µV²/Hz) plotted against frequency (Hz) from 0 to 120 Hz. Each colored line represents a different EEG channel, as shown in the electrode layout on the top right. The high power at low frequencies, especially below 20 Hz, reflects the strong influence of low-frequency brain rhythms. Unlike filtered EEG, this unfiltered data shows additional spectral features, including subtle variations across channels and a noticeable peak around 60 Hz, likely due to power line noise. The power generally decreases at higher frequencies, with some fluctuations that may indicate muscle or environmental artifacts. This frequency distribution captures both brain activity and noise, making it useful for studying brainwave characteristics in their raw form, relevant for applications like brainwave-based authentication.

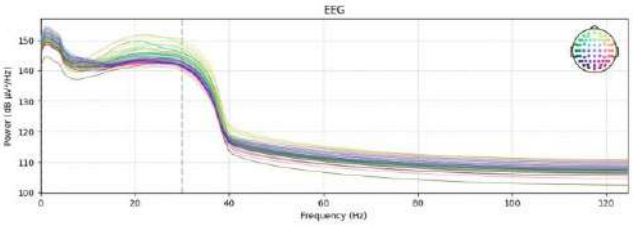

Figure 4.2. Power Spectral Density (PSD) for Filtered EEG Data

The figure shows the power spectral density of filtered EEG signals across multiple channels, with power (dB µV²/Hz) plotted against frequency (Hz) from 0 to 120 Hz. Each line represents an EEG channel, as shown in the electrode layout on the top right. The high power seen at low frequencies, especially below 20 Hz, gradually drops around 40 Hz, marked by a dashed line, then continues to decrease at higher frequencies. This trend is typical of EEG data, where low frequencies (delta, theta, alpha) dominate in power and reflect cognitive and resting states, while higher frequencies (beta, gamma) are less pronounced. This frequency distribution helps in analyzing brain activity and is valuable for identifying unique brainwave patterns, supporting applications like brainwave-based authentication.

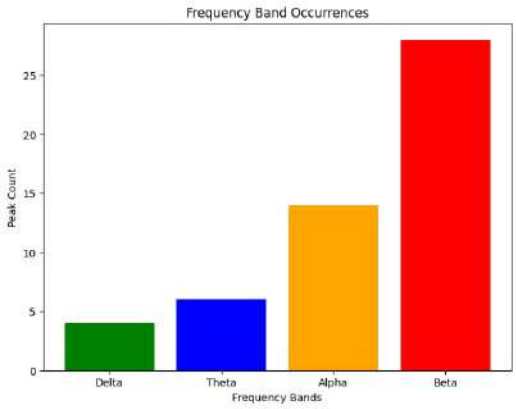

Figure 4.3. Frequency Band Occurrences

The figure shows that beta frequency band occurrences are the highest, indicating that the brain is in a more active or alert state. This is consistent with event-related potentials (ERPs), as beta waves, typically within the 13-30 Hz range, are often associated with enhanced cognitive function, concentration, and awareness, particularly during attention-demanding tasks [50].

4.1.2 Importance of Event-Related Potentials (ERP) in Authentication

Event-Related Potentials (ERPs) are crucial components in EEG-based authentication systems as they provide distinct brainwave responses to specific sensory stimuli. [48] Studies show that ERP features are highly discriminative, revealing unique responses from individual neural circuits, making them suitable for reliable biometric use. Furthermore, ERP captures high-level cognitive functions such as attention and memory, which support its stability and accuracy in identifying unique brainwave patterns across individuals [49].

In this study, we focused on ERPs triggered by auditory, visual, and somatosensory stimuli to isolate unique neural signatures. ERPs are advantageous because they capture automatic neural reactions to stimuli, which are less influenced by conscious control, making them difficult to replicate or falsify.

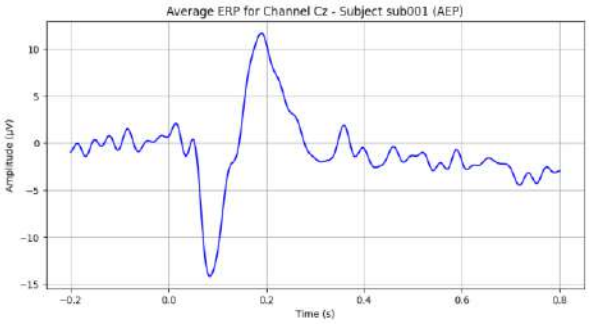

Figure 4.4. Average Event-Related Potential (ERP) of Participant 1 (AEP).

The figure above displays the Average Event-Related Potential (ERP) for channel Cz of Subject "sub001" in response to an Auditory Evoked Potential (AEP) task. The x-axis shows time in seconds, centered around the stimulus onset at 0 seconds, while the y-axis represents the amplitude in microvolts (µV). A notable negative deflection occurs shortly after stimulus onset, followed by a strong positive peak around 0.2 seconds (200 ms), which is characteristic of typical AEP responses. This pattern indicates the brain's electrical response to auditory stimuli, where initial negative and subsequent positive peaks are expected. The data suggests that this participant exhibits a strong and clear ERP response to the auditory stimulus, commonly analyzed in studies of sensory processing and cognitive function.

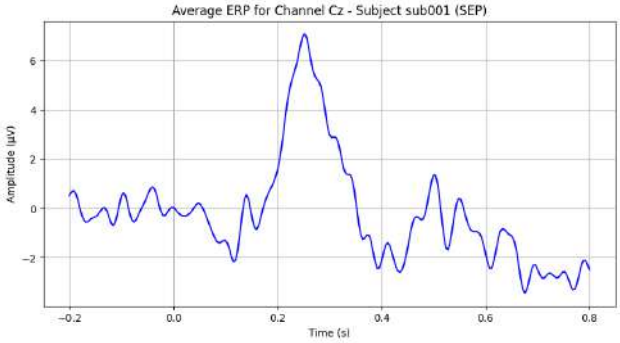

Figure 4.5. Average Event-Related Potential (ERP) of Participant 2 (SEP).

The figure shows the average Event-Related Potential (ERP) waveform from Channel Cz for Subject "sub001" during a Somatosensory Evoked Potential (SEP) task. Time (in seconds) is represented along the x-axis, with 0 marking the stimulus onset. The y-axis shows the amplitude of the ERP in microvolts (µV). A prominent positive peak appears at around 0.2 seconds post-stimulus, likely representing the P200 component, which reflects early sensory processing in response to the stimulus. This peak, reaching approximately 6 µV, indicates a strong sensory response. Following the P200, smaller positive and negative deflections appear, possibly indicating later cognitive processes, such as attention and evaluation. Overall, the waveform highlights the brain's sensory processing stages and responsiveness to the SEP task.

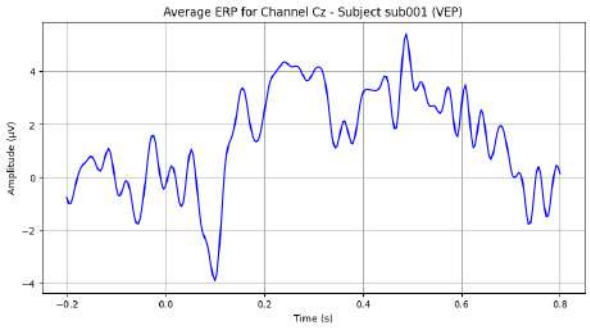

Figure 4.6. Average Event-Related Potential (ERP) of Participant 3 (VEP).

The figure displays the Event-Related Potential (ERP) for Channel Cz in Subject sub001 during a Visual Evoked Potential (VEP) task, capturing the brain's response to visual stimuli over time. Channel Cz, positioned at the top center of the head, records general cortical responses, with the y-axis showing amplitude in microvolts (µV) and the x-axis representing time from a pre-stimulus baseline (-0.2s) to 0.8 seconds after stimulus onset. Immediately after

the visual stimulus (at 0 seconds), an initial dip occurs, indicating early sensory processing, followed by prominent peaks around 0.3 and 0.5 seconds, reflecting perceptual and attentional processing stages. The waveform then gradually diminishes between 0.5 and 0.8 seconds, marking the end of the brain's primary response. This ERP waveform provides insight into the neural processing stages involved in Subject sub001's response to visual stimuli, which is valuable for comparing individual brainwave patterns in brainwave-based authentication studies.

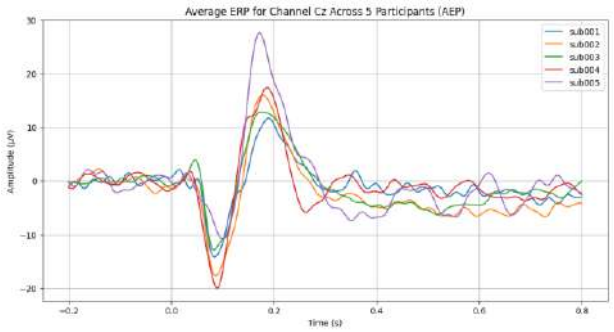

Figure 4.7. Average Event-Related Potential (ERP) Across 5 Participants (AEP).

In this graph, the averaged responses of five participants during an AEP task reveal both shared and unique features. While the general waveform shape—such as a prominent peak and trough around similar time points—reflects typical auditory evoked response patterns, each participant's ERP exhibits subtle, distinguishing characteristics. These individual differences appear in the timing and amplitude of peaks, as well as in the overall waveform shape, even under the same task conditions. Such unique features are consistent enough to differentiate participants, highlighting how ERP data, despite showing similar response structures across subjects, contain participant-specific signatures.

4.2 Brainwave Authentication System Evaluation

4.2.1 CNN-SVM Initial Model

The initial CNN model was developed as a baseline for the brainwave authentication system without using automated hyperparameter tuning. The model achieved training accuracy of 99% and validation accuracy of 75%, which suggested issues with overfitting as the model is performing very well only at the training set. The model's structure consisted of only convolutional layers, pooling layers and batch normalization without specific configuration to generalize effectively across unseen data.

Table 4.1. CNN model initial layers

Hyperparameter	Initial Value
Conv2d_1	8
Conv2d_2	16
Conv2d_3	32
Learning Rate	0.0001

Table 4.1 shows the initial CNN model proposed by the researchers with three convolutional layers starting from 8, 16, and 32. The filter size of the layers are all 3x3 with batch normalization and max pooling (2x2 pool size) for all the three convolutional layers.

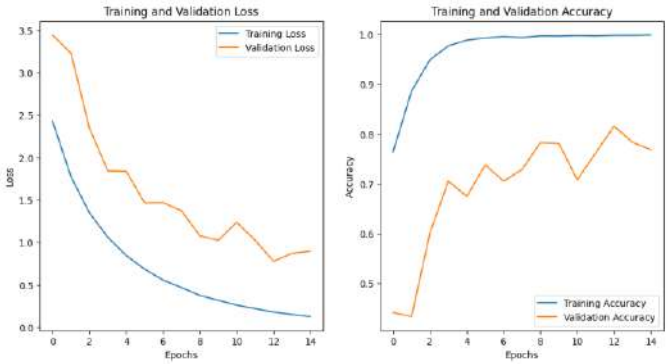

Figure 4.8. Graph of Initial CNN Training/Validation Loss and Accuracy

The initial model as shown in the figure is performing well on training data reaching 99.87% accuracy and 13.36%. However, the validation set only reached its highest validation accuracy of 76% that started from 44.12% on epoch 1 indicating overfitting to training data. Moreover, manually changing of hyperparameters was conducted in the initial cnn-svm model by the researchers. In addition, the loss for both training data and validation is consistently improving across epochs.

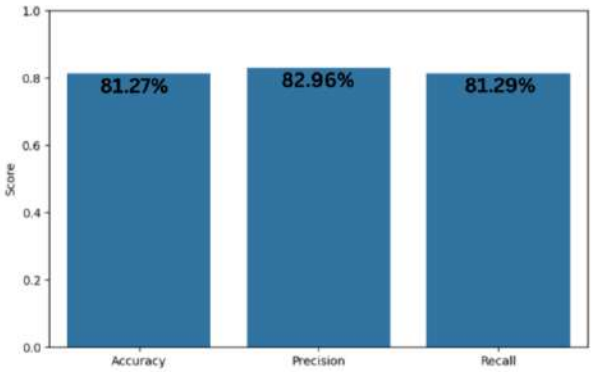

Figure 4.9. Initial CNN-SVM's Metrics on accuracy, precision and recall

Figure above shows the accuracy, precision and recall metrics of the initial cnn-svm model reaching 81% - 82% across the three metrics. These results indicate that the cnn-svm model is feasible to continue if the authentication system fails. These findings emphasized the need of fine-tuning the hyperparameters to enhance the model's accuracy to unseen data. Due to this, the researcher opted for an automated hyperparameter tuning approach using Hyperband, with the goal of optimizing the hyperparameters to effectively classify subjects in the brainwave authentication system.

4.1.2 Fine-Tuned CNN-SVM Model

To optimize the CNN-SVM model architecture, the researchers utilized Hyperband Keras tuner for hyperparameter searching, aiming to maximize validation accuracy by trying ranges of CNN configurations. Through this fine-tuning and after 30 trials, the hyperparameter tuning achieved a validation accuracy of 97% with a similar range of training accuracy of 96%.

Table 4.2. Fine-tuned CNN-SVM Architecture after hyperparameter tuning

Hyperparameter	Best Value
Conv2d_1	56
Conv2d_2	56
Conv2d_3	16
Dense Layer	72
Dropout Rate	0.43000000000000005
L2 Regularization_1	0.07100000000000001
L2 Regularization_2	0.09999999999999999
Learning Rate	0.00033904359243909244

Table 4.2 showed the optimized hyperparameters allowing the model to generalize across the validation data. Increasing the validation filter sizes in convolutional layers enabled the model to capture more intricate features in the EEG signals across different subjects. Introduction of L2 regularization to the first and third convolution layers and a dropout improved the model by reducing overfitting.

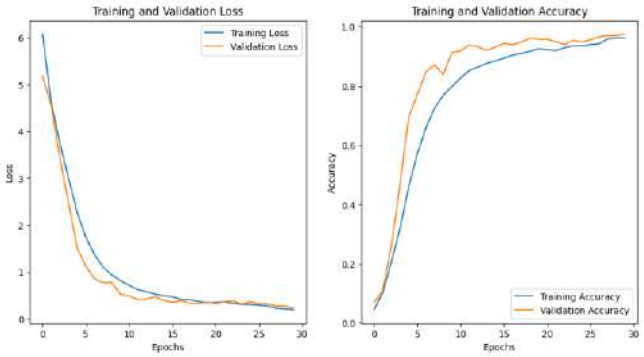

Figure 4.10. Graph of Fine-tuned Training/Validation Loss and Accuracy

After implementing the best hyperparameters, the CNN model achieved an improved validation accuracy of 97%, indicating a successful optimization. Training and validation loss curves as seen on Figure 4.8 illustrate a trend where the training and validation loss decreases steadily across the epochs while both accuracy are increasing over 30 epochs.

Table 4.3. SVM Model configuration as the classifier

SVM Model	Configuration
Kernel	Radial Basis Function
C	1.0
Gamma	Scale

After training the CNN as a feature extractor, Support Vector Machine (SVM) will be the classifier on the extracted features. SVM's kernel is radial basis function (rbf) where it allows to create complex decision boundaries to data that isn't linearly separable similar to the complex features of each subject's EEG. The regularization parameter C allows a smoother decision boundary to achieve generalized separation of classes. Lastly, the gamma helps in reaching an optimized result by calculating based on the data itself.

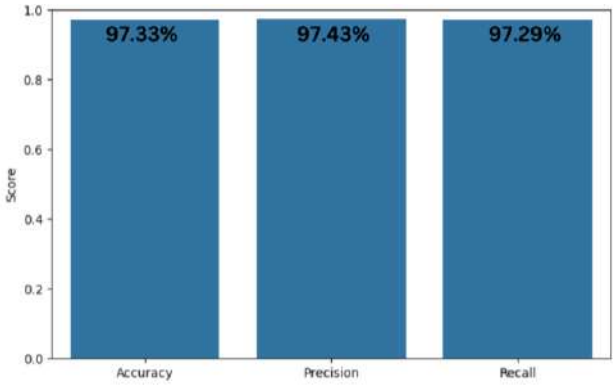

Figure 4.11. Fine-tuned CNN-SVM's Metrics on accuracy, precision and recall

Figure 4.11 shows that the CNN-SVM model reached 97% on accuracy, precision and recall. This indicates that the model correctly classifies most of the subject's EEG recording and predicts the correct subject corresponding to the EEG datapoint. Moreover, a high precision means the model has the ability to limit false positives predicting the EEG recording with high confidence. On its recall, it demonstrates the ability to detect true positives, capturing the specific patterns of each subject in the data and predict correctly.

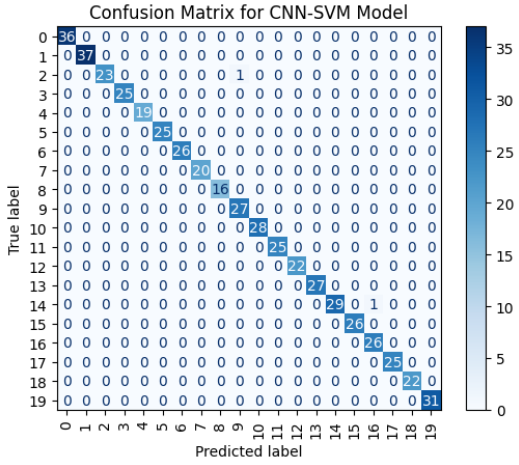

Figure 4.12. CNN-SVM model confusion matrix for the first 20 classes

To further evaluate the CNN-SVM model's performance on different classes for each subject, the confusion matrix on figure 4.12 was generated. Note that the figure above was only for the first 20 classes out of 85. The matrix reveals that the model aligns well with the true labels with some incorrect classifications across the classes.

Table 4.4 Classification report of the CNN-SVM model

Class	Precision	Recall	F1-score	Support
0	1.00	1.00	1.00	36
1	1.00	0.95	0.97	39
2	1.00	0.92	0.96	25
3	0.96	1.00	0.98	25
4	0.95	0.95	0.95	20
5	1.00	0.96	0.98	26
6	1.00	1.00	1.00	26
7	0.95	0.91	0.93	22
8	0.94	0.84	0.89	19
9	0.96	0.96	0.96	28
10	1.00	1.00	1.00	28
11	1.00	1.00	1.00	25
12	1.00	1.00	1.00	22
13	1.00	0.90	0.95	30
14	0.94	0.88	0.91	33
15	0.93	1.00	0.96	26
16	0.96	1.00	0.98	26
17	0.96	0.96	0.96	26
18	1.00	0.92	0.96	24
19	1.00	1.00	1.00	31
20	0.97	1.00	0.99	35
21	0.85	1.00	0.92	23
22	0.85	0.92	0.88	2
23	1.00	0.98	0.99	40
24	1.00	1.00	1.00	32
25	0.97	1.00	0.99	33
26	1.00	1.00	1.00	31
27	1.00	0.97	0.99	34
28	1.00	1.00	1.00	25
29	1.00	1.00	1.00	31
30	1.00	1.00	1.00	26
31	1.00	1.00	1.00	29

32	0.97	1.00	0.98	32
33	1.00	1.00	1.00	33
34	1.00	1.00	1.00	29
35	0.87	0.93	0.90	28
36	1.00	0.94	0.97	16
37	0.96	1.00	0.98	24
38	0.83	0.93	0.88	27
39	0.97	0.94	0.96	34
40	1.00	1.00	1.00	35
41	0.95	1.00	0.98	39
42	1.00	1.00	1.00	26
43	1.00	1.00	1.00	38
44	1.00	1.00	1.00	22
45	1.00	1.00	1.00	32
46	1.00	0.90	0.95	29
47	1.00	0.96	0.98	23
48	1.00	1.00	1.00	30
49	1.00	0.97	0.98	33
50	1.00	1.00	1.00	31
51	0.88	0.91	0.89	32
52	0.97	1.00	0.98	30
53	1.00	0.79	0.89	34
54	0.90	1.00	0.95	26
55	1.00	1.00	1.00	40
56	0.97	0.97	0.97	32
57	0.97	1.00	0.98	32
58	1.00	0.96	0.98	23
59	1.00	0.96	0.98	28
60	0.94	0.89	0.91	35
61	1.00	1.00	1.00	28
62	1.00	1.00	1.00	21
63	0.74	0.90	0.81	31
64	0.97	1.00	0.98	32
65	0.97	1.00	0.98	32
66	1.00	1.00	1.00	19
67	1.00	1.00	1.00	34
68	1.00	1.00	1.00	30
69	0.97	1.00	0.98	29
70	1.00	1.00	1.00	22
71	1.00	0.96	0.98	26
72	1.00	1.00	1.00	30
73	0.95	0.95	0.95	22
74	1.00	1.00	1.00	26
75	1.00	0.94	0.97	33
76	0.93	0.96	0.95	27
77	1.00	1.00	1.00	27
78	1.00	1.00	1.00	23
79	1.00	1.00	1.00	29
80	0.96	1.00	0.98	23
81	1.00	1.00	1.00	33
82	0.96	0.93	0.95	29
83	1.00	1.00	1.00	36
84	1.00	1.00	1.00	21
accuracy	0.97	0.97	0.97	0.97
macro avg	0.97	0.97	0.97	2436
weighted avg	0.98	0.97	0.97	2436

Table 4.4 classification report summarizes the CNN-SVM model in classifying the subject for their EEG recording in the test set. The class 0-84 corresponds to each subject in the dataset with class 0 representing subject 1 and so on. Per-class metrics achieved high results indicating that the model correctly predicts for each class consistently. To emphasize the model's performance, the recall of most of the class are ranging from 0.9 to 1.0 showing that the model correctly predicts all instances of the class with missing only a small fraction of each sample class. Similarly, f-1 score demonstrates that the for each class cnn-svm model shows excellent performance with no misclassification on most of the class.

Furthermore, the metrics below the table shows the accuracy, macro average and weighted average. On its evaluation, accuracy, precision, and recall achieved a consistent 97% across the metrics indicating that the model performs consistently well across classes with only minor misclassification in terms of performance.

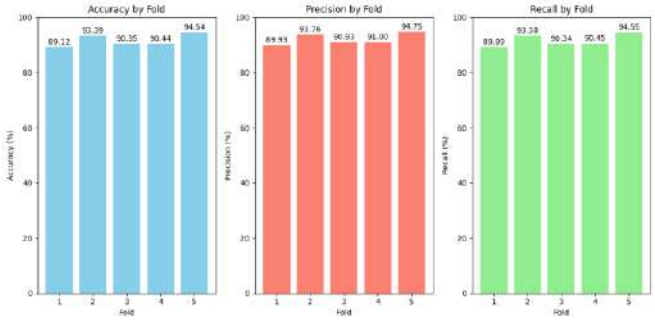

Figure 4.13. Cross Validation metrics by fold

For an in-depth assessment of the authentication system, stratified k-fold cross validation was conducted with the goal of evaluating the model's accuracy, precision, and

recall. By dividing the dataset into equally distributed subsets, the model can be evaluated without potential bias for each class. In the 5-fold cross validation, all the classes have the same proportion as the original dataset and will give significant metrics on different folds of the dataset.
Figure 4.13 displayed the result metrics after 5 fold of cross validation. The accuracy ranges from 89.12% to 94.54% across five folds indicating that the model consistently performs well in correct prediction of the class.

Precision by fold graph presents the similar result ranging from 89.93% and 94.75% showing its high precision in identifying true positive instances. With this precision, the model is able to maximize in predicting correct class leading to true positives and minimizing wrong prediction leading to false positives. The high precision means that the authentication system ensures that unauthorized users are rejected most of the time in the system.
Lastly, recall by fold graph assesses the model's ability to correctly identify all samples of each class. As seen from the graph the recall is consistent across five folds starting from 89.09% in the first fold and reaching 94.55% recall in the fifth fold. This high recall demonstrates the model's capability to capture true positive and accepting registered users.

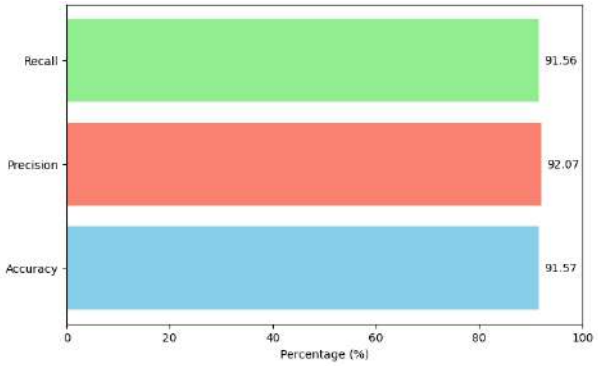

Figure 4.14. Cross Validation average metrics by fold

Despite minor fluctuations in some folds, the model consistently achieves high accuracy, precision, and recall. To add with the cross validation results, figure 4.14 shows the graph of the average metrics of accuracy, precision, and recall after five folds. Mean recall of 91.56% showcases the model's ability to reliably authenticate registered users in all samples of that class in cross validation.The mean precision of 92.07% establishes the model's success in minimizing false positives which is important in an authentication system. 91.57% mean accuracy reveals the overall reliability of the authentication system across five folds.

4.3 Authenticate Users With Their Brainwave And Reject Intruders

4.3.1 Model Performance in Authenticating and Rejecting

EEG files used for knowing the model performance are from the testing set which is another set, not from the training set from session 1. This model has demonstrated strong performance in yielding a high accuracy of correctly classifying registered users and effectively rejecting intruders. Although it produces an accuracy of 97.12%, precision of 97.39%, and recall of 97.12%, thereby reliably identifying registered users, ensuring that when accepted, the user is highly likely to be correct, it also successfully detects most registered users without rejecting them falsely, and false negatives are at a minimal rate. False positives are very low or nonexistent, which means intruders get rejected. Notably, the intruder, `sub086`, which contains EEG files which were combined from five intruder subjects for convenience, was correctly accepted by most repetitions, meaning that the model tends to identify a violator in its vast majority of repetitions. Overall, the model is very effective at authenticating legitimate users and rejecting intruders.

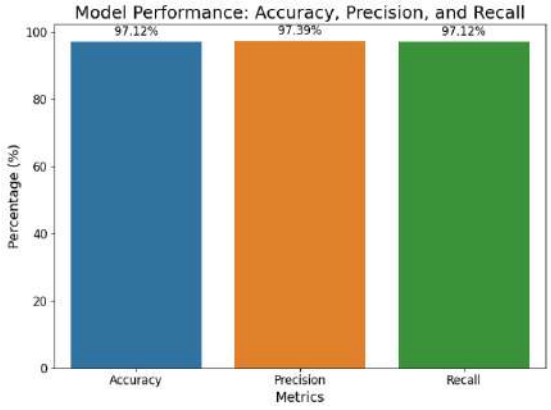

Figure 4.15. Evaluation of Model Performance: Accuracy, Precision, and Recall for Session 1

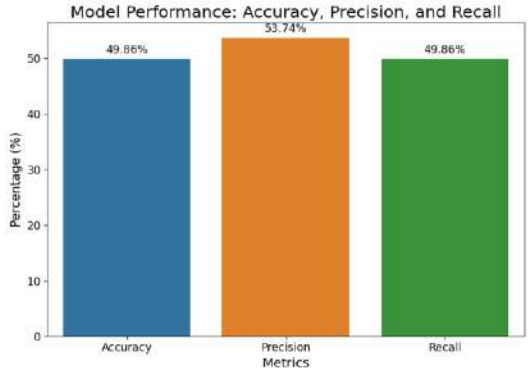

Figure 4.16. Evaluation of Model Performance: Accuracy, Precision, and Recall for Session 2

In Session 2, the model's performance on the data which are only subjects sub001 to sub020. All measures were low: accuracy at 49.86%, precision at 53.74%, and recall at 49.86%. True positives are how many correctly it identified instances out of 720 with a figure of 359, while actual positives are how many it wrongly identified as false negatives with a count of 361 out of 720.

4.3.2 Overall Classification Metrics for Registered and Intruder Users

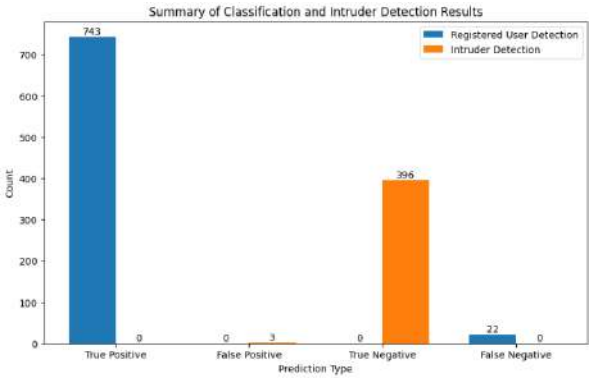

Figure 4.17. Summary of Classification and Intruder Detection Results for Session 1

The system correctly accepted 743 legitimate epochs across each registered user (sub001–sub085) as True Positives but refused 22 legitimate epochs, rejecting them wrongly (False Negatives) a total of 765 legitimate epochs. There were zero False Positives in the case of legitimate epochs; in other words, the system does not mistake a legitimate epoch for an intruder.

A correctly rejected 396 intruder epochs from intruder (sub086) as True Negatives and accepted in error 3 intruder epochs as False Positives a total of 396 intruder epochs. Overall performance is good, although the system may be further improved to reduce the acceptance of intruder epochs.

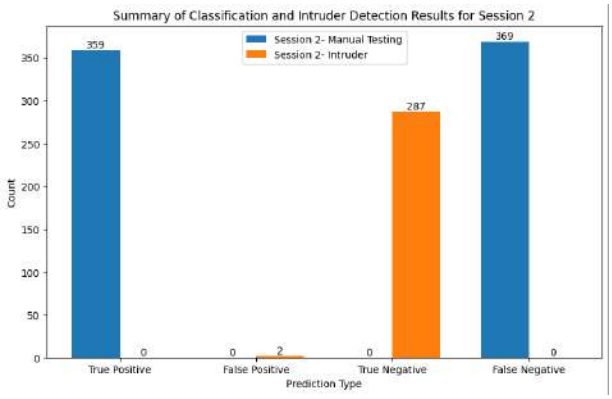

Figure 4.18. Summary of Classification and Intruder Detection Results for Session 2

The system captured 359 epochs across users correctly as True Positives for Session 2. It mistakenly rejected 369 legitimate epochs as False Negatives, amounting to a total of 720 legitimate epochs (Figure 4.18).

For intruder detection, the system correctly rejected 287 epochs of intruders as True Negatives and falsely accepted only 2 epochs of intruder as False Positives out of 289 epochs. Overall, the system shows a high requirement for improvement, especially to reduce False Negatives among epochs of legitimate behavior for increasing detection accuracy.

4.3.3 Confidence Score Analysis

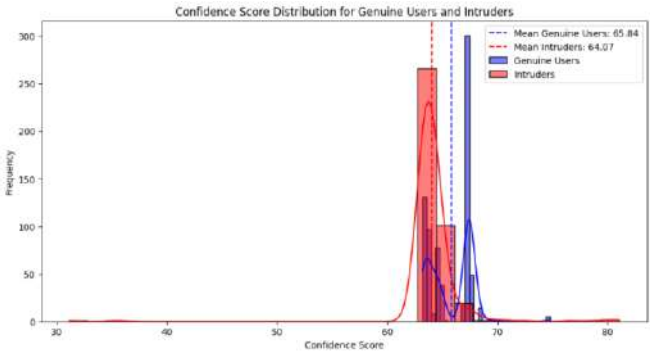

Figure 4.19. Distribution of Confidence Scores of Registered Users and Intruders for Session 1

As seen in the graph, the confidence scores of registered users versus intruder users are quite close. This is because of the effort of the CNN-SVM model to fit the intruder users into the classes that exist inside the model. Therefore, a first layer of protection is needed, such as making the user state their subject identity to identify who they are when logging in. This figure shows a plot of the confidence scores of both the registered users (blue) and intruders (red) obtained with frequency histograms over each group. It indicates that the mean confidence score is 65.84 for the

true users, which is very close to being greater than for intruders, about 64.07. That is, the system is, on average, slightly more confident while classifying the true users. These histograms allow for a direct comparison of such distributions so that, although the confidence scores of both groups are close, the slight difference in means is visible, and this difference helps to understand whether the system is able to distinguish the two groups based on confidence levels.

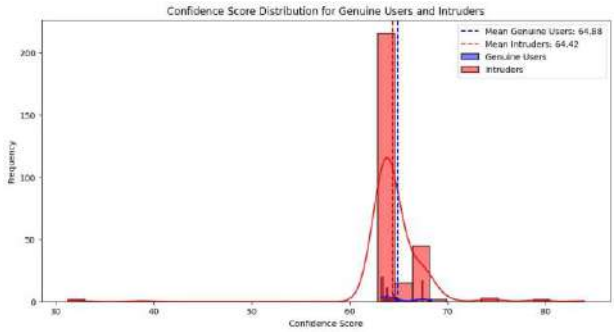

Figure 4.20. Distribution of Confidence Scores of Registered Users and Intruders for Session 2

The plot shows the distribution of confidence scores for legitimate users versus intruders in Session 2; registered users are colored in blue, and intruders in red. Their confidence scores range similarly; they almost have the same means—64.88 for legitimate users and 64.42 for intruders. This overlap implies that the CNN-SVM model is not distinguished properly to differentiate between legitimate users and intruders, and it would be very hard to classify which was which solely based on confidence score.
The histograms indicated this challenge because the distributions can be regarded as very nearly aligned.

4.3.4 Histogram of Registered Users vs Intruders

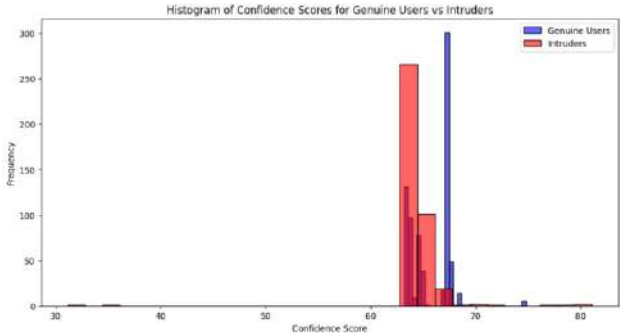

Figure 4.21. Histogram of Confidence Scores of Registered Users vs. Intruders for Session 1

This plot overlays the histograms of the confidence scores for genuine users in blue and intruders in red, mapping x to represent the confidence score and y to depict how often a score is reached. This kind of plot tells a story through visualized distribution about how the-confidence scores of genuine versus intruder users are distributed, thus showing the capabilities of the model in the differentiation of the two. The overlapping histograms are helpful in judging the central tendencies and spread of both groups' confidence scores.

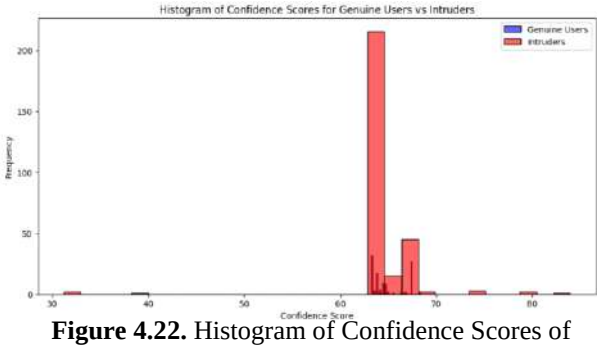

Figure 4.22. Histogram of Confidence Scores of Registered Users vs. Intruders for Session 2

This plot over-plot the histograms of the confidence scores for the genuine users (blue) and intruders (red), where the x-axis is the confidence scores, and the y-axis is the frequency for each score. Although the plot is designed to present the score distribution of both groups, the blue bars for the actual users are the worst, while the red bars for intruders dominate the graph. This would indicate that the confidence scores of intruders are more spread out or only appear in limited ranges and hence more observable. Histograms overlapped with each other provide a good feeling of how close the confidence scores of both classes are to each other, which suggests that the model fails to distinguish between real users and intruders using confidence scores alone.

4.4 Evaluating System Performance Through Authentication Metrics

To evaluate the performance and accuracy of our brainwave authentication system, we used three core metrics: False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). These metrics reveal how well our system can distinguish authorized users from intruders and maintain a balance between security and usability.

4.4.1 Metrics Calculation (Session-1)

1) **False Acceptance Rate (FAR)**: FAR measures the likelihood of unauthorized users being accepted as legitimate users.

- Formula:

$$FAR = \frac{\text{False Positive}}{\text{False Positive + True Negative}} \times 100\%$$

- Calculation: In the intruder-testing folder, we observed 3 false positives and 396 true negatives. Thus,

$$FAR = \frac{3}{3 + 396} \times 100\% = 0.75\%$$

2) **False Rejection Rate (FRR)**: FRR quantifies the probability that legitimate users are incorrectly denied access.

- Formula:

$$FRR = \frac{\text{False Negative}}{\text{False Negative + True Positive}} \times 100\%$$

- Calculation: In the manual-testing folder, 743 instances were correctly accepted as authorized users, while 22 were incorrectly rejected, resulting in an FRR of:

$$FRR = \frac{22}{743 + 22} \times 100\% = 2.88\%$$

3) **Equal Error Rate (EER)**: EER is the rate at which FAR and FRR converge. This point represents the ideal operating threshold of the system, balancing security and accessibility.

- Calculation: Based on the results from Session-1, the EER lies near the operating points for the observed FAR of **0.75%** and FRR of **2.88%**, indicating a strong balance between false acceptances and rejections.

4.4.2 Significance of Calculated Values (Session-1)

- **FAR of 0.75%**: This low FAR signifies that only a small percentage of unauthorized attempts result in mistaken access, demonstrating the system's effectiveness in guarding against unauthorized users. In real-world scenarios, a low FAR is crucial for maintaining security, as it minimizes the risk of intruders gaining access.

- **FRR of 2.88%**: The relatively low FRR indicates that only a small portion of legitimate users are rejected. This value highlights the system's efficiency in allowing access to valid users with minimal inconvenience. A low FRR is essential for a user-friendly experience, as frequent rejections can frustrate legitimate users and reduce usability.

- **EER Balance**: The closeness of FAR and FRR at the current operating point illustrates that the system achieves a balanced performance, making it suitable for applications that demand both high security and high accessibility.

4.4.3 Metrics Calculation (Session-2)

1) **False Acceptance Rate (FAR)**: FAR measures the likelihood that unauthorized users are incorrectly accepted as legitimate users by the system.

- Formula:

$$FAR = \frac{\text{False Positive}}{\text{False Positive + True Negative}} \times 100\%$$

- Calculation: In the intruder-testing folder, we observed 2 false positives and 287 true negatives. Thus, the FAR is calculated as follows:

$$FAR = \frac{2}{2 + 287} \times 100 = 0.69\%$$

2) **False Rejection Rate (FRR)**: FRR quantifies the probability that legitimate users are incorrectly denied access to the system.

- Formula:

$$FRR = \frac{\text{False Negative}}{\text{False Negative + True Positive}} \times 100\%$$

- Calculation:

$$FRR = \frac{361}{361 + 359} \times 100 = 50.14\%$$

3) **Equal Error Rate (EER)**: EER represents the point where the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are equal, reflecting the threshold at which security and accessibility are balanced.

- Calculation: Based on the results from Session-2, we calculated the FAR to be **0.69%** and the FRR to be **50.14%**. While these two metrics do not yet converge at the same point in this session, the EER would be somewhere between these values, reflecting a need for further optimization in balancing false acceptances and rejections.

4.4.4 Significance of Calculated Values (Session-2)

- **FAR of 0.69%**: This very low FAR indicates that the likelihood of unauthorized users being accepted as legitimate is extremely small. A FAR of 0.69% demonstrates that the system is effective in rejecting false positives, making it highly secure in preventing unauthorized access. This is particularly important in real-world scenarios where high security is crucial to prevent unauthorized individuals from gaining access.
- **FRR of 50.14%**: The relatively high FRR of 50.14% suggests that a significant portion of legitimate users were incorrectly rejected during authentication. While a low FAR is essential for security, this higher FRR indicates that there may be challenges with the system's user-friendliness. A high FRR could lead to user frustration, as legitimate users may experience repeated rejections. This trade-off between security and usability needs to be addressed for an optimal user experience.
- **EER Balance**: The disparity between FAR and FRR in this session reflects an imbalance between security and accessibility. While the system is highly effective in rejecting unauthorized users (low FAR), it struggles with correctly accepting legitimate users (high FRR). This indicates that further tuning of the system's threshold might be necessary to achieve a better balance, ensuring that security is maintained without overly burdening legitimate users. The system's performance in Session-2 suggests room for improvement in balancing both security and usability.

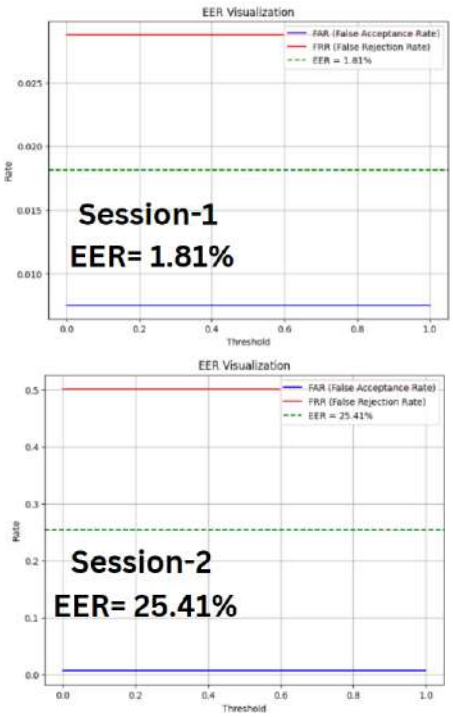

Figure 4.23. Equal Error Rate (EER) Visualization

The graph displays the Equal Error Rate (EER), a key metric in evaluating biometric system accuracy. Along the x-axis, we have the threshold values, which determine the confidence level needed to confirm a match. The y-axis represents the error rates, specifically the False Acceptance Rate (FAR) and False Rejection Rate (FRR). Where the FAR and FRR curves intersect, we find the EER, marking the threshold at which the system has an equal probability of mistakenly accepting an unauthorized user or rejecting a legitimate one. Systems with a lower EER are generally more accurate and reliable, as they maintain a better balance between security and accessibility.

For Session 1, the EER is 1.81% at a specific threshold, indicating a low probability of error. This suggests a highly accurate and reliable biometric system. In contrast, Session 2 has an EER of 25.41%, indicating a significantly higher chance of error and a less reliable system. Lower EER values generally signify better system performance.

4.4.5 Comparison of Authentication Performance Metrics with Existing Studies

In this study, we achieved a remarkably low False Acceptance Rate (FAR) of 0.75% in Session-1, indicating a minimal likelihood of unauthorized access, thereby enhancing the security of the authentication system. This FAR falls below the recommended thresholds noted in Arias-Cabarcos et al. (2023), which suggest maintaining FAR close to 1% or lower for secure applications [47]. Additionally, our Session-1 FAR is slightly lower than the values reported by Yousefi & Kolivand (2023), who achieved FARs of 0.17 for Support Vector Machine (SVM) and 0.15 for Neural Network (NN) classifiers in their brainwave-based authentication system using deep breathing [15]. These comparisons underscore the effectiveness of our method in minimizing unauthorized access, a crucial aspect for any high-security system.

For **Session-2**, our system achieved a similar FAR of 0.69%, again underscoring the system's ability to effectively prevent unauthorized access. This rate continues to align well within secure application standards and remains competitive with the FAR metrics noted in related studies. The consistent low FAR across both sessions reaffirms the robustness of our system's security measures, especially in comparison with the secure thresholds advocated in previous literature.

Our False Rejection Rate (FRR) in **Session-1** was recorded at 2.88%, which, while slightly higher than the exceptionally low FRR values of 0.02 for SVM and 0.03 for NN reported by Yousefi & Kolivand [15], remains effective and meets standards for accessibility in secure authentication systems. Notably, Arias-Cabarcos et al. (2023) discuss the usability-security trade-off, observing that very low FAR values may often lead to increased FRR [47]. In contrast, our balanced FAR and FRR effectively mitigate this trade-off in Session-1, ensuring both high security and a positive user experience.

In **Session-2**, however, we observed a higher FRR of 50.14%, suggesting a significant trade-off between usability and security. This elevated FRR indicates that some challenges remain in maintaining a low rejection rate for legitimate users while prioritizing security. Compared to the notably low FRR values observed in related studies, our Session-2 FRR points to potential areas for improvement in optimizing system performance without compromising ease of access.

These combined FAR and FRR values across both sessions suggest that while **Session-1** achieves a strong Equal Error Rate (EER), **Session-2** may require additional tuning to achieve a similar balance. Our findings are consistent with the usability-security trade-off noted by Arias-Cabarcos et al. (2023) and reflect that certain session-specific factors might impact system accuracy and accessibility. Overall, while **Session-1** positions our system as competitive with established biometric authentication systems, **Session-2** results indicate opportunities for fine-tuning to enhance performance consistency.

This analysis, alongside the findings of Yousefi & Kolivand (2023) and Arias-Cabarcos et al. (2023), highlights the efficacy of brainwave-based authentication methods in balancing FAR and FRR to achieve robust security and ease of access [15], [47]. Our system demonstrates strong security capabilities across sessions, establishing it as a valuable contribution to biometric authentication research, with further potential for session-specific optimizations.

CHAPTER V

Conclusion & Recommendation

5.1 Summary of Findings

The main purpose of the study is to develop an authentication model that is capable of accepting registered users and rejecting intruders. By using convolutional neural network (CNN) as feature extractor and support vector machine (SVM) as classifier the goal is achieved through the evaluation of the model.

- The study demonstrated the potential of brainwave based authentication utilizing the reaction of the subject in a task stimulus as a biometric factor. By using distinct ERP features, the system captured unique responses from subjects. Using preprocessing of EEG recording, isolated the frequency band and ERP that contributed to the accuracy of the model.

- The initial CNN-SVM model achieved 75% validation accuracy which reflects overfitting. By using hyperband keras-tuner the model's metrics were improved reaching 97% accuracy, precision, and recall. The model correctly classifies users while limiting false positives and negatives.

- Using stratified k-fold cross validation, the system proved its consistency and reliability across five folds with accuracy ranging from 89.12% to 94.54%. Precision and recall averaged 92.07% and 91.56%, respectively showcasing the model's performance across different subsets of the dataset.

- The system excelled in identifying and accepting registered users while rejecting intruders during testing. Session 1 achieved 97.12% with low FAR

of 0.75% and FRR of 2.88%. On the other hand, session 2 presented challenges with an FRR of 50.14% indicating difficulties in user acceptance due to session-specific factors and limited training of user's EEG recording on session 2. Despite this, the system maintained a low FAR of 0.69% making its effectiveness in rejecting unauthorized access acceptable.

- Equal Error Rate (EER) highlighted the balance between security and stability of rejecting and accepting users. Session 1 achieved optimal alignment of FAR and FRR while session 2 requires optimization due to higher FRR.

5.2 Conclusion

With the ever growing development of technology, ensuring the security of sensitive information in the digital world is important. Security methods like passwords and two factor authentication are vulnerable to replication and brute-forcing. Biometric authentication offers a promising solution using the user's organic characteristics like its physiological or behavioral traits. Among these, using the brain activity of a user provides a way for a personalized and robust form of security.

Through this research, the authors successfully developed a brainwave-based authentication using EEG signals particularly event-related potential (ERP) which is the user's unique response to a task stimulus. The result shows that the distinguishable feature of ERP patterns can be a biometric factor for secure authentication. By using CNN-SVM model, the system achieved a high level of accuracy proving the ability of EEG signals for user authentication in real-world applications.

Despite challenges such as session variability and environmental noise, the result shows the feasibility of using an EEG-based authentication. The system achieved a low false acceptance rate (FAR) and false rejection rate (FRR) demonstrating its ability to have consistent performance on session 1. On the other hand, session 2 highlighted areas for improvement and the need for an improved model allowing classification of users across sessions. The insights from the study contribute to the realm of security, specifically biometrics offering a foundation in the country for future studies to build upon. With further optimization, EEG-based systems can be used for high-security environments where knowledge-based password is not enough. This work not only demonstrates the potential of biometrics but also paves the way for advancements in EEG-based authentication.

5.3 Recommendation

This research study reveals the potential of EEG signals as a way for biometrics. Building on the insights gained from this research, several recommendations can guide future enhancements in EEG-based authentication.

- Incorporate regular calibration across different sessions to account for variability of user's EEG signals ensuring system's consistency.
- Integrate brainwave-based authentication with other biometric modalities to enhance user verification and authentication
- Develop affordable, compact and comfortable EEG device to enable convenient authentication for real-world scenario
- Conduct independent EEG data collection for future research to remove dataset constraints and ensure consistent recording techniques and controlled environments.

References:

[1] Grigutyte M. (2023). What is user authentication, and why is it important?. NordVPN. Retrieved from https://nordvpn.com/blog/what-is-user-authentication/

[2]Barney N. (2023). Definition authentication. TechTarget. Retrieved from https://www.techtarget.com/searchsecurity/definition/authentication

[3]Aratek (2023). The top 8 benefits of biometrics in cybersecurity. Retrieved from https://www.aratek.co/news/the-top-8-benefits-of-biometrics-in-cybersecurity

[4]Nedap Security (2023). Is biometric security something to consider for your access control system?. Retrieved from https://www.nedapsecurity.com/insight/biometric-security/#:~:text=One%20of%20the%20key%20benefits,be%20used%20for%20multifactor%20verification.

[5]Pathak A. (2023). Unlocking the future: how is brain wave authentication is transforming security. Medium. Retrieved from https://medium.com/@pathakanuj807/unlocking-the-future-how-brain-wave-authentication-is-transforming-security-f053743e7fe7

[6] (Bak & Jeong, 2023). When Does Your Brain Know You? Segment Length and Its Impact on EEG-based Biometric Authentication Accuracy. Retrieved from https://arxiv.org/pdf/2403.12644.

[7] Maayan G., (2021). User authentication methods that can prevent the next breach. Retrieved from https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/

[8] A. Pathak, "How Brainwave Authentication Works," *J. Adv. Authent. Technol.*, vol. 7, no. 3, pp. 112-125, 2023.

[9] K. Hulick, "Utilization of EEG in Authentication Systems," *IEEE Trans. Biometrics Security*, vol. 5, no. 2, pp. 45-58, 2023.

[10] R. Schomp, "Individuality in EEG Patterns," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 8, no. 3, pp. 215-228, 2020.

[11] J. Sooriyaarachchi, S. Seneviratne, K. Thilakarathna, and A. Zomaya, "Genetic Influence on Brain Structure and Function," *IEEE J. Sel. Top. Signal Process.*, vol. 14, no. 1, pp. 102-115, 2020.

[12] Y. Soni, S. Somani, and V. Shete, "Impact of Visual and Auditory Stimuli on EEG-Based Authentication," *IEEE Trans. Cybernetics*, vol. 6, no. 2, pp. 321-334, 2017.

[13] TajDini, M., Sokolov, V., Kuzminykh, I., & Ghita, B. (2023). Brainwave-based authentication using features fusion. Computers & Security, 129, 103198. https://doi.org/10.1016/j.cose.2023.10319

[14] Schomp, R. (2020). Behavioral Biometric Security: Brainwave Authentication Methods. https://doi.org/10.17615/r7bn-df89

[15] Yousefi F. & Kolivand H. (2023). A robust brain pattern for brain-based authentication methods using deep breath. Computers & Security 135 (2023) 103520. https://doi.org/10.1016/j.cose.2023.103520.

[16] Arias-Cabarcos, P., Habrich, T., Becker, K., Becker, C., & Strufe, T. (2021). Inexpensive Brainwave Authentication: New techniques and insights on user acceptance. USENIX. https://www.usenix.org/conference/usenixsecurity21/presentation/arias-cabarcos

[17] Tron Baraku, Christos Stergiadis, Simos Veloudis, Manousos A. Klados, Personalized user authentication system using wireless EEG headset and machine learning, Brain Organoid and Systems Neuroscience Journal, Volume 2,2024, Pages 17-22,ISSN 2949-9216, https://doi.org/10.1016/j.bosn.2024.03.003.

[18] Sooriyaarachchi J., Seneviratne S., Thilakarathna K., & Zomaya A (2020). MusicID: a brainwave-based user authentication system for internet of things. Retrieved from https://arxiv.org/abs/2006.01751.

[19] Soni Y., Somani S., & Shete V. (2017). Biometric user authentication using brain waves. 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2016, pp. 1-6, doi: 10.1109/INVENTIVE.2016.7824888.

[20] Abhang, P. A., Gawali, B. W., & Mehrotra, S. C. (2016). Technological basics of EEG recording and operation of apparatus. In Elsevier eBooks (pp. 19–50). https://doi.org/10.1016/b978-0-12-804490-2.00002-6

[21] Bidgoly, A. J., Bidgoly, H. J., & Arezoumand, Z. (2020). A survey on methods and challenges in EEG based authentication. Computers & Security, 93, 101788. https://doi.org/10.1016/j.cose.2020.101788

[22] Yaribeygi, H., Panahi, Y., Sahraei, H., Johnston, T. P., & Sahebkar, A. (2017, January 1). The impact of stress on body function: A review. PubMed. https://doi.org/10.17179/excli2017-480

[23] Sjamsudin, F.P. (2017, January 30). EEG-based Authentication with Machine Learning. https://core.ac.uk/download/pdf/144465828.pdf

[24] TajDini, M., Sokolov, V., Kuzminykh, I., & Ghita, B. (2023). Brainwave-based authentication using feature fusion. https://www.sciencedirect.com/science/article/pii/S0167404823001086

[25] Hagen, E., Magnusson, S. H., Einevoll, G. T. & Cook, E. P. (2022). Brain signal predictions from multi-scale networks using a linearized framework. bioRxiv. https://www.biorxiv.org/content/10.1101/2022.02.28.482256v3.full.pdf

[26] Alipio, M. I. (2022, January 29). Development, evaluation, and analysis of biometric-based bank vault user authentication system through brainwaves. Journal of Ambient Intelligence & Humanized Computing/Journal of

Ambient Intelligence and Humanized Computing. https://doi.org/10.1007/s12652-021-03679-8
[27] Herradura T, Cordel M. (2023). Exploring the Relationship between EEG
Features of Basic and Academic Emotions. Philipp J Sci 152(4): 1507–1516.
https://doi.org/10.56899/152.04.19
[28] Yaribeygi, H., Panahi, Y., Sahraei, H., Johnston, T. P., & Sahebkar, A. (2017). The impact of stress on body function: A review. EXCLI Journal, 16(1), 1057–1072. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5579396/
[29] Li, X., Fan, H., Wang, H., & Wang, L. (2019). Common spatial patterns combined with phase synchronization information for classification of EEG signals. Biomedical Signal Processing and Control, 52, 248–256. https://doi.org/10.1016/j.bspc.2019.04.034

[30] P. Tangkraingkij, A. Montaphan, & I. Nakavisute. (2017). An appropriate number of neurons in a hidden layer for personal authentication using delta brainwave signals. https://doi.org/10.1109/iccre.2017.7935076
[31] Mihajlovic, V., et al. (2015). Improving the reliability of EEG-based biometric systems. *IEEE Transactions on Information Forensics and Security*.
[32] Marcel, S., & Millán, J. del R. (2007). Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*.
[33] M.V. Ruiz-Blondet, Z. Jin, S. Laszlo Cerebre: a novel method for very high accuracy event-related potential biometric identification IEEE Trans. Inf. Forensics Secur., 11 (7) (2016), pp. 1618-1629
[34] Palaniappan, R. (2008). Using EEG signals for authentication purposes: Challenges and solutions. *Biometrics Research Journal*
[35] Polich, J. (2007). Updating P300: An integrative theory of P3a and P3b. Clinical Neurophysiology.
[36] Huang, G., Hu, Z., Chen, W., Zhang, S., Liang, Z., Li, L., Zhang, L., & Zhang, Z. (2022). M3CV: A multi-subject, multi-session, and multi-task database for EEG-based biometrics challenge. NeuroImage, 264, 119666. https://doi.org/10.1016/j.neuroimage.2022.119666
[37] Creel, D. (2012). **Visually evoked potentials.** Webvision - NCBI Bookshelf. https://www.ncbi.nlm.nih.gov/books/NBK107218/

[38] Klingner, C. M., & Witte, O. W. (2018). **Somatosensory deficits.** In Handbook of clinical neurology (pp. 185–206). https://doi.org/10.1016/b978-0-444-63622-5.00009-7
[39] Roser, P., Kawohl, W., & Juckel, G. (2020). **The loudness dependence of auditory evoked potentials as an electrophysiological marker of central serotonergic neurotransmission: Implications for clinical psychiatry and psychopharmacotherapy.** In Handbook of behavioral neuroscience (pp. 361–374). https://doi.org/10.1016/b978-0-444-64125-0.00020-7
[40] Maiorana, E., (2021b). Transfer learning for EEG-based biometric verification. In: IEEE
International Conference on Bioinformatics and Biomedicine (BIBM). BIBM 2021,
pp. 3656–3661. doi:10.1109/BIBM52615.2021.9669495.
[41] Bidgoly, A.J., Bidgoly, H.J., Arezoumand, Z., (2022). Towards a universal and
privacy preserving EEG-based authentication system. Sci. Rep. 12, 1–12.
doi:10.1038/s41598-022-06527-7.
[42] Kang, J.H., Jo, Y.C., Kim, S.P., (2018). Electroencephalographic feature evaluation for improving personal authentication performance. Neurocomputing 287, 93–101.
doi:10.1016/j.neucom.2018.01.074.
[43] Toledo-Pérez DC, Rodríguez-Reséndiz J, Gómez-Loenzo RA, Jauregui-Correa JC. (2019). Support Vector Machine-Based EMG Signal Classification Techniques: A Review. Applied Sciences. 2019; 9(20):4402. https://doi.org/10.3390/app9204402
[44] McCarthy J. (2018). Re-rethinking Recommendation Engines: Psychology and the Influence of False Negatives. Retrieved from https://gumption.typepad.com/blog/2008/02/re-rethinking-r.html

[45] Easycap (n.d). Easycap Electrode Layouts based on 10%-System. Retrieved from https://www.easycap.de/wp-content/uploads/2018/02/Easycap-10-based-electrode-layouts.pdf
[46] Gan Huang, Zhenxing Hu, Weize Chen, Shaorong Zhang, Zhen Liang, Linling Li, Li Zhang, Zhiguo Zhang. (2022). M3CV: A multi-subject, multi-session, and multi-task database for EEG-based biometrics challenge. NeuroImage. Volume 264. ISSN 1053-8119. https://doi.org/10.1016/j.neuroimage.2022.119666.
[47] Arias-Cabarcos, P., Fallahi, M., Habrich, T., Schulze, K., Becker, C., & Strufe, T. (2023). Performance and Usability Evaluation of Brainwave Authentication Techniques with Consumer Devices. *ACM Transactions on Privacy and Security*, *26*(3), 1–36. https://doi.org/10.1145/3579356
[48] Sabeti, M., Boostani, R., & Moradi, E. (2020). Event related potential (ERP) as a reliable biometric indicator: A comparative approach. *Array*, *6*, 100026. https://doi.org/10.1016/j.array.2020.100026
[49] Armstrong, B. C., Ruiz-Blondet, M. V., Khalifian, N., Kurtz, K. J., Jin, Z., & Laszlo, S. (2015, October). Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics. https://www.sciencedirect.com/science/article/abs/pii/S0925231215004725
[50] Hendrayana, Y., Kusumah Negara, J. D., Nuryadi, Gumilar, A., & Lesyiana, M. (2020). The impact of beta

brain waves in improving cognitive function through brain jogging applications. *International Journal of Human Movement and Sports Sciences*, *8*(6A), 73-77. http://www.hrpub.org
[51] Z. Mao, W. X. Yao and Y. Huang, "EEG-based biometric identification with deep learning," 2017 8th International IEEE/EMBS Conference on Neural Engineering (NER), Shanghai, China, 2017, pp. 609-612, doi: 10.1109/NER.2017.8008425.
[52] Zhang S, Sun L, Mao X, Hu C, Liu P. Review on EEG-Based Authentication Technology. Comput Intell Neurosci. 2021 Dec 24;2021:5229576. doi: 10.1155/2021/5229576. PMID: 34976039; PMCID: PMC8720016.