Behavioral Biometric Security: Brainwave Authentication Methods

Rachel Schomp
The University of North Carolina at Chapel Hill
Department of Computer Science

Abstract—**This paper investigates the possibility of creating an authentication system based on the measurements of the human brain. Discussed throughout will be an evaluation of the feasibility of brainwave authentication based on brain anatomy and behavior characteristics, conventional vs. dynamic authentication methods, the possibility of continuous authentication, and biometric ethical and security concerns.**

I. INTRODUCTION

Technology continues to permeate our daily lives, and with this expansion comes increasing cyber security concerns. Simple PINs and passwords are no longer enough to limit use to only the intended user. More complex means of authentication are required, and the way this can be accomplished is through behavior-based biometric security. With approximately 100 billion neurons [17], each brain is identifiably unique in the way it reacts to and processes incoming information. It is this characteristic that can turn brainwaves into an authentication metric. However, neurological information is a growing and critical information class. The commerciality of neural devices is a contributing factor to this expansion with neural implants for clinical patients, at-home neurostimulators, and Brain-Computer Interfacing smartphone applications. A multitude of new access points carrying neural information has now been established and this continued multiplication in data extraction will lead to great strides in behavioral-biometrics, but also inevitable security and privacy concerns [28].

II. THE BRAIN

"If the human brain were so simple
That we could understand it,
We would be so simple
That we couldn't."
- Emerson M. Pugh [52]

At the center of human cognition is the brain, an electrochemical organ capable of generating as much as 10 watts of electrical power [76]. The brain is comprised of approximately 100 billion nerve cells known as neurons and is a complex system where mental states emerge from interactions between many functional and physical levels [17]. It can process immense amounts of information, and with such a complex structure, no one has yet to decrypt the whole picture on how precisely the brain works. Research suggests that at some point, the computational power of a computer will surpass that of the human brain. However, as we do not yet know how the entire brain computes, there is no finite answer for exactly how fast the brain works [63]. Despite the daunting complexity of this organ, growing an understanding of the brain is imperative to cracking authentication methods using brainwaves.

Similar to the gates and wires of a computer, the neurons in a brain gather and transmit electrochemical signals [19]. This electrical activity emanating from the brain manifests in the form of brainwaves. Brainwaves fall into four main categories—Beta waves, Alpha waves, Theta waves, and Delta waves [76].

i. Beta waves occur when the brain is actively engaged in mental activities such as a person who is in active conversation. As the fastest of these brainwaves, Beta waves can be characterized as having a relatively low amplitude and frequency between 15 to 40 cycles per second.
ii. A person who has just finished a task and sits down to rest would be in an Alpha state. Alpha waves are slower and higher in amplitude, and describe a non-arousal state.
iii. Theta waves are most common in a state where the task being completed has become so automatic you disengage from being mentally focused on it. One example of this is when you are driving on the highway

and discover you can no longer remember your actions or thoughts for the last five miles. Theta waves often occur when individuals are running outside or in a state of mental relaxation such as in the shower; you are more prone to the flow of ideas in this category.

iv. Finally, Delta waves are classified as having the greatest amplitude and slowest frequency between 1.5 and 4 cycles per second. They will never go completely down to zero because that would indicate brain death, but deep dreamless sleep will take you down to the lowest frequency of approximately 2 cycles per second [25].

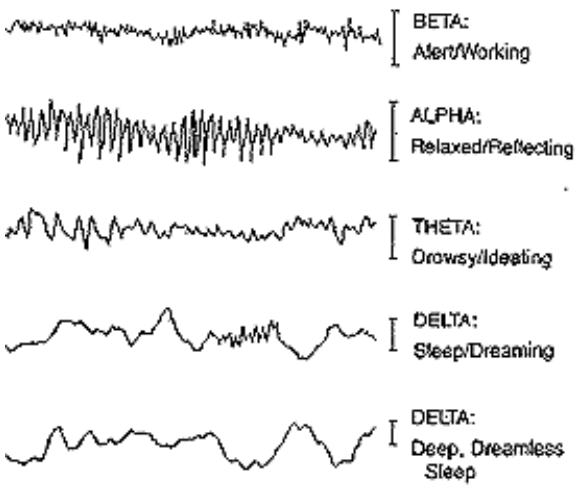

Figure 1: From Ned Herrmann [76]

What is unique about brainwaves is that every man, woman, and child of all ages, backgrounds, and daily lives experience the same brainwave characteristics. These categories and interactions are consistent across geographical lines and cultural differences [76].

III. BRAIN-COMPUTER INTERFACES

This section will discuss Brain-Computer Interface devices before moving on to specific types of Brain-Computer Interfaces (I), and the Electroencephalograph (II).

Brain-Computer Interface (BCI) devices are predicted to become heavily used in the future for applications in user authentication, neuro-medical tools, entertainment and gaming, and smartphones [18]. BCIs establish a communication pathway for the user to either send information to or control an external device exclusively through brain activity [23]. This action bypasses the muscle and peripheral nervous systems, making it a useful tool for people who do not have full function of their bodies. In clinical settings, BCI applications include repairing, augmenting or assisting cognitive functions, and sensory-motor functions in patients with physical impairments. Given the significant potential of BCI devices, particularly the commerciality of immediacy and hands-free controls, Yuan et al. [80] predicts BCIs will gradually replace device control mechanisms, including the keyboard, touch screen, and voice command.

I. TYPES OF BCIS

Brain-Computer Interfaces are divided into three types: invasive, partially-invasive, and non-invasive [17].

i. Invasive BCIs require the neural device to be implanted directly into the gray matter—the outer layer of the brain. Invasive BCIs could also include the surgical implantation of an electrode array, which connects directly to the central nervous system [23].

ii. Partially-invasive BCI devices are placed inside the skull, but do not touch the gray matter. Rather, the device is likely situated in one of the dura matter layers.

iii. Non-invasive BCI devices are attached directly to the scalp, requiring no surgical action. This option is the most common for practical authentication devices involving brainwaves [23].

Various types of signals can be used in a BCI. Particularly, neural activity produces magnetic and metabolic signals in addition to the more common electrical activity captured in an Electroencephalograph (EEG) [44]. Magnetic fields can be recorded with a Magnetoencephalography (MEG), and the metabolic activity of the brain can be observed through a Positron Emission Tomography (PET) scan. Other possibilities include the Functional Magnetic Resonance Imaging (fMRI) and Optical Imaging. Despite the numerous options to gather information on brain signals, none are as accessible for authentication as the EEG, as it requires no sophisticated techniques or an exorbitantly expensive

device in specialized facilities such as a hospital [44].

II. ELECTROENCEPHALOGRAPH

The small electrical charges created by the approximately 100 billion neurons in the brain contribute to the generation of an electric field with electrical potentials fluctuating around the scalp [17]. This electric output can then be read and dissected by an Electroencephalograph machine. An EEG records and measures the brain's electrical activity through voltage fluctuations resulting from ionic current with the neurons [75] through electrodes placed on the skin [5]. These signals are the output that represents brain activity based on a person's unique neural pathway patterns. The uniqueness of these signals is what makes user-specific brainwaves challenging to recreate as they can be made distinct from the mood, mental state, and genetic makeup of the user. Such electrophysiological traits also naturally allow detecting whether the subject is alive at the time of attempted authentication. This is an additional security measure afforded to behavioral biometrics connected to consciousness that static biometrics systems, such as fingerprint and palm print, do not possess [24].

EEG-biometry requires modeling or classifying of the extracted EEG features from the collected signals from the scalp channels. These scalp signals, however, are not the source signals inside the brain. An EEG is the summation of synchronous signal activity among thousands of neurons; thus, signals read may not have come from the location of the node. To obtain a more accurate reading from specific sites, spatial filtering can be used during the extraction phase [71]. It is more likely that the signal is a noisy and linear mixture of the components emanating from the brain [24]. This reveals a limiting factor for the success of EEG-based biometrics, as a linear mixture matrix can be sensitive to where the EEG nodes are precisely placed on the scalp.

EEG signals are generally analyzed in two separate ways: frequency domain and time domain [4].

i. Frequency domain focuses on the separation of oscillatory signals based on different bands such as alpha, beta, etc.
ii. Time domain involves the averaging of the signals at the onset of a particular event. These signals that are averaged in a synchronized fashion are called Event-Related Potentials (ERP).

ERPs represent different components of the processes of human perception and cognition; they are the brain's time-locked response to stimulus [18]. ERPs are useful because they increase the signal-to-noise ratio, thus reducing the unrelated brain activity shown. Due to the noisiness of readings from the brain, finding a measurement that minimizes this is crucial for a more transparent reading in authentication. Also, EEGs and ERPs are non-volitional, which states the user cannot willingly control them, making these metrics difficult to be compromised [18].

These analyses can be implemented to derive the unique brainwave fingerprint of an individual user [18]. The advantages afforded by collecting brainwaves through an EEG is the accessibility and ease with which it can acquire the data. It can capture quality temporal resolution and is relatively tolerant of subject movement [68]. All of these benefits are in addition to being non-invasive through external electrode placement. Commercial-grade devices are even now readily available making this form of authentication both safe and feasible.

IV. AUTHENTICATION

This section will contain information on basic forms of authentication such as passwords and PINs (I). It will then discuss what biometric authentication entails and how matches are made (II). Finally, it will cover biometric authentication possibilities using brainwaves (III).

I. BASIC FORMS OF AUTHENTICATION

Means of authentication come in four distinct forms commonly described as something you know, have, are or do. Something you know or have are the most common types of authentication means with passwords, PINS, and electronic key cards being the preferred methods [78]. In password-based authentication, the password serves to authenticate the ID, which in turn provides security by determining whether the user is authorized to gain access to the system, and what privileges should be given to the user. The ID is used in what is called discretionary access control [78]. A considerable amount of people use the same password across multiple

online login platforms (*Figure 2)*. This indicates that although users have the choice to create highly complex and varied passwords for any device or system, users often choose to re-use passwords from other accounts. Given the constrictive password parameters set by certain sites, users might be inclined to create a single complex password that will always satisfy the majority of site requirements. Remembering this single password across online logins can be easier than remembering multiple complex passwords; thus, the vulnerabilities with textual passwords is apparent.

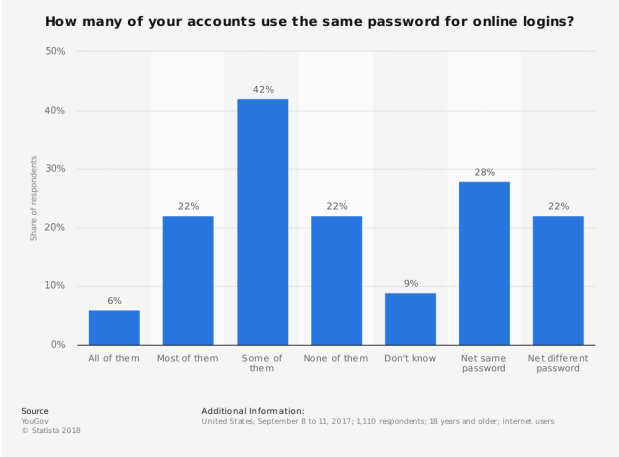

Figure 2: From YouGov [79]

Periodically changing passwords is a way to counteract the security issues from re-using passwords. However, the higher the frequency of forced password change, the less likely users are to remember them [54]. This leads to users writing down passwords or storing them in files to keep up with the change, an additional security problem.

Some vulnerability concerns with passwords include an offline dictionary attack, password guessing, shoulder surfing, and workstation hijacking. An offline dictionary attack occurs when someone gains access to the system password file and compares the password hashes against hashes of commonly used passwords. If users create passwords that are relatively common such as "qwerty", "password", or even common words, this attack could offer the adversary access. One countermeasure against this would be to include controls that prevent the password file from being accessed without authorization through intrusion detection. However, if those measures failed, the attacker would have access to all of the hashed passwords [78]. With the example of password guessing against a single user, if the attacker has any personal information about the user, they could use that to guess the password. Training people to choose long and difficult passwords acts as a countermeasure against this attack, but it still does not offer the depth of assurance in the security of the system other authentication methods could provide. Finally, some of the more important vulnerabilities for this paper that password authentication possess are shoulder surfing and workstation hijacking. Shoulder surfing occurs when someone can view the user typing in his or her password, thus being able to access the system later. As brainwaves are not able to be "viewed" by an onlooker, brainwave authentication is a method that could be immune to this type of attack. Workstation hijacking occurs when the attacker waits until a logged-in station is unattended and subsequently can use the system after this vacancy. Although traditional countermeasures for this would be to automatically log-out the user after a certain period of inactivity, in the future, continuous behavioral biometrics could solve this problem.

II. BIOMETRIC AUTHENTICATION

Another method for authentication fall under the biometric category, with something you are or something you do. Biometrics can be further split into two factions, static and dynamic. Static biometrics would include fingerprints, iris scanning, and facial recognition. Possibly more advanced forms of security are dynamic biometrics with voice pattern recognition, typing rhythm, gate analysis, and eventually brainwave-based authentication. Fingerprints can easily be stolen and replicated with standard imaging and software, making this biometric, although the most widely used and accessible at the moment, also easily broken. Consumers are far more comfortable with static biometric security systems, particularly with fingerprint scanning accounting for 53% of consumers (*Figure 3)*. Although only approximately 10% of consumers preferred behavioral biometrics, considering the relative immaturity of this development, this indicates there could be consumer acceptability for behavioral biometrics in the future.

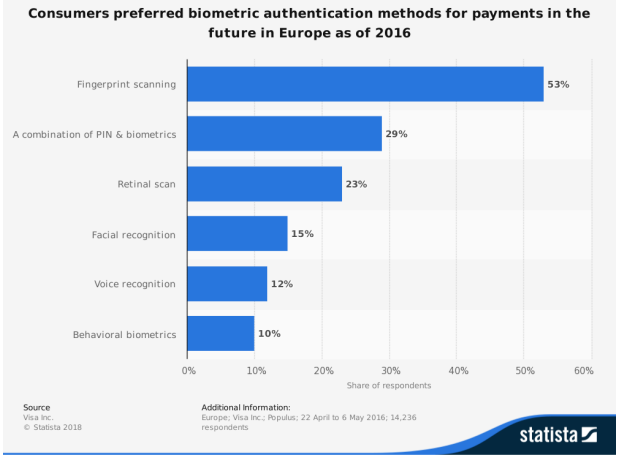

Figure 3: From Visa Inc. [74]

Biometric accuracy is imperative to the success of a system. Because the data being used is so complex, it would be naïve to expect an exact match [78]. Constituting the element of accuracy is the False Match Rate (FMR) and False Non-Match Rate (FNMR) (*Figure 4)*. The FMR is the frequency with which biometric samples from various sources are erroneously assessed to be from the same source. An example of this would be if a fingerprint from someone who should not be granted access is mistakenly found to be a match, and granted access to the system. FNMR describes the frequency with which samples from the same source are incorrectly assessed to be from different sources. Similar to the example above, if fingerprints from a person with access rights were presented for authentication, but the system evaluated the fingerprints to not be the same as the template, this would indicate a False Non-match.

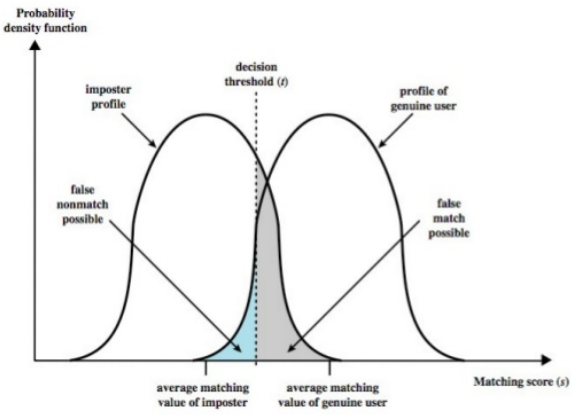

Figure 4: From William et al. [78]

III. BRAINWAVE AUTHENTICATION

One of the main concerns regarding the validity of brainwaves as a practical authentication method is whether people have distinct brainwaves, similar to how no two fingerprints are the same. This question was first addressed in the 1960's by Vogel F. who discovered there was a connection between one's genetic code, DNA, and one's EEG signals [17]. This was tested with monozygotic (identical) twins, who were shown to possess the same EEG patterns regardless of the situation. This revealed that unlike fingerprints, brainwaves are connected to the genetic code, and people may have similarities in the way their brains function. Despite the fact that brainwaves are not as distinctive among identical twins, for the majority of the population, brainwaves are as different as fingerprints, and thus a candidate for a new form of authentication.

For a method of biometric authentication to be considered valid and efficient, it must address seven predetermined requirements—universality, distinctiveness, permanence, collectability, performance, acceptability, and circumvention [17].

Universality – Every person required to use the system should possess the feature required for authentication. Since every human has a brain and assuming they are the one trying to access the system, the possession of this living organ provides universality.

Distinctiveness – This raises the question whether this feature can be unique among all individuals. As mentioned in the prior paragraph, brainwaves are unique among different people except for similar patterns between identical twins. Brainwaves are not as 100% distinctive as fingerprints, but the complexity of the brain is undeniable.

Permanence – The feature of authentication should not change significantly over time to meet the requirement of permanence [17]. Because of how humans process and store memories relating to our experiences, brainwaves will reflect a person's unique psychological state. Brainwave signals are generated, however, when someone accesses their semantic memories rather than episodic memories [25]. Semantic memories do not change drastically over time, with neurons likely behaving the same as before. Episodic memories remember our experiences; for instance, if you get scratched by a cat, the next time you read the word "cat", the episodic memory neurons that fire will likely be different.

Semantic memories record the definitions of particular words [25]. This collection of meanings we accumulate and associate with words can subtly differ from person to person, thus providing an individual pattern. Despite the relative stability of brainwaves during a stage in someone's life, our brains do change as we experience more, gain knowledge, and eventually start to forget. Brainwaves will never be as permanent as conventional static methods of authentication and will require an authentication system that adapts to the changes that occur throughout a lifetime.

Collectability and Performance – Moving to the points of collectability and performance, new equipment such as portable and mobile-enabled EEG headsets are making the collection of brainwaves easier than ever. This bodes well for the collectability of this metric while making sure the performance of these models is quick and accurate.

Acceptability – With any new technology acceptability might be low in the initial stages, but as the use of new authentication measures gains traction, acceptability could grow.

Circumvention – Finally, circumvention is perhaps one of the most important considerations for an authentication system. As mentioned above regarding the distinctiveness of brainwaves, the brain is highly complex, and it would be tough for an imposter to mimic someone else's brainwave pattern [25].

Despite the attributes brainwaves might fulfill, practical applications of brainwave authentication systems are not currently widespread, as the accuracy has yet to reach 100% [60] reliably. Although there have been a few reports of achieving 100% accuracy [38], most research studies fall in the accuracy range of 96-98% [1, 4, 50, 55].

V. EEG-BASED AUTHENTICATION MODEL

The foundation of an EEG-based authentication system includes three main phases—data collection, feature extraction, and classification. Data collection occurs through the capture of EEG signals as measured by the electrodes placed on the scalp. This will happen while the user is performing a specific mental task such as thinking of a word, imagining movement, or recognizing an image. This data collection is the first step in gathering enough information to create a biometric template.

The next phase is feature extraction, which can be difficult with the amount of noise in the readings of brainwaves. Some algorithms used to extract signal features include Power Spectral Density, Fast Fourier Transform, and Discrete Wavelet Transform [61]. One authentication problem is extracting high-entropy information from the user to find what makes a person unique. Certain areas of the brain develop more based on training, education, and experience. An example of this can be found in professional musicians; string musicians are known to have larger somatosensory cortical areas associated with the fingers [15]. It is also known that alpha frequency brainwaves can have considerable variability between people [14]. It is this variability that implies how different signals can be emitted from the brain even when two people are thinking of the same thing. Through the extract, some of this dimensionality and variability of signals is lost to get the most accurate data. This can create a problem for the classification phase. Reduction in data variability, although it helps with classification, also simplifies the features, making it easier for an adversary to manufacture false biometric data to feed the system [61].

In the classification section, a trained classifier outputs a matching score suggesting how closely a feature vector resembles a member of a particular class; this is likely based on a predetermined threshold [61]. Deep learning techniques are shown to provide high classification accuracies and can detect latent features from raw data [70]. Sophisticated deep learning methods such as the convolutional neural networks [32] and recurrent neural networks [77] can be implemented to reduce dependency on the feature extraction phase. Deep neural networks are comprised of several stacked layers of neurons which helps improve the performance of the network [32]. Each layer is trained on a distinct set of features which depends on the output from the previous layer. Moving further into the layers allows for the training on complex features. Because deep learning methods can be applied with minimal to no feature extraction, desired features are automatically learned by the network. This makes deep learning suitable for cases when the desired features are unknown, as is the case with the complex data emitted by the brain [70].

I. PASS-THOUGHTS

One form of brainwave authentication involves

the use of pass-thoughts, an authentication method by merely thinking of a password, or reacting to a stimulus [18]. Pass-thoughts are seen as superior to passwords or PINs that must be typed in because they are not vulnerable to dictionary attacks or shoulder surfing. The potential size of space in a pass-thought system seems to be unbounded in theory, as there are no real bounds on human thought; however, constraints would have to be placed on the system itself [71]. If the assumption is made that each neuron in a human brain could store only one bit of information, pass-thoughts could produce keys of 2^{36} bits in size. In spite of this math, the theoretical entropy is much higher as neurons are so complex there has yet to be a complete model of the capabilities of individual neuron behavior [71].

Brainwave authentication via pass-thoughts is a mix of behavioral biometrics and the "what you know" section of authentication mechanisms. This is because a user would essentially be repeating a pre-set password, PIN, or image, which is something he or she would know, but it would be done via an EEG reading, hence the biometric component. A potential authentication system using pass-thoughts was presented by Thorpe et al. [71]. The user would begin by pressing a key to indicate they are ready to begin the authentication process and then think of their previously chosen pass-thought before pressing another button indicating they are done. Pass-thoughts would undergo feature extraction; however, there is no need to translate the brain signals. Given that this translation is one of the most challenging parts of BCI research, pass-thoughts could be a simpler beginning model for brainwave authentication methods.

Pass-thought authentication could use a multitude of stimuli including textual and graphical. Entire sentences, a picture, or memory could serve as a password, eliminating the single word passwords most people use. Particularly unique about pass-thoughts is the opportunities with graphical passwords as an alternative to textual passwords, motivated by the remarkable ability of human memory for pictures. Many graphical password schemes have emerged in research such as Recognition-based graphical password schemes with Deja Vu [13, 51]. Pass-thoughts have been tested in brainwave authentication studies in conjunction with other metrics to create a multimodal system. These systems have been shown to have accuracy of 99% [31]. However, authentication with only pass-thoughts [60] found pass-thoughts alone only offered 8% accuracy.

II. EVENT-RELATED POTENTIALS

A more promising angle for pass-thought authentication is to focus on P300 signal detection. A P300 signal can be registered by a BCI device and is an ERP component which can be elicited during the process of decision making [16] and appears approximately 300ms after an exciting or surprising event [71] (*Figure 5)*. By randomly highlighting elements on a screen during the authentication process, spikes in a P300 signal silently record recognition that could be checked against the template to see if it matches. This scheme allows for use of images, letter sequences, or even musical riffs. This would, however, take a slightly longer amount of time to complete, as P300 approaches have a bit rate of 4.8 characters per minute to have 90% accuracy [71].

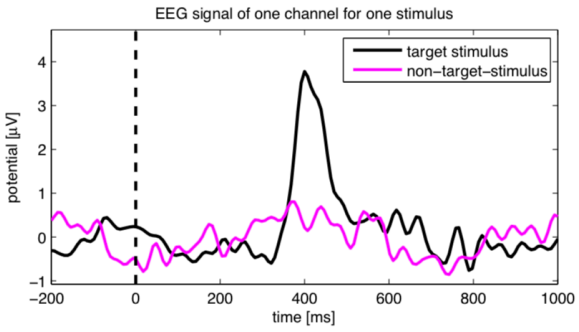

Figure 5: From Martinovic et al. [45]

One study conducted by Ruiz-Blondet et al. [60] used an ERP biometric protocol called "CEREBRE" designed to elicit distinct responses. In this research study, it is argued that using ERPs is the most effective means for authentication with the brain. Because ERPs are created through the averaging over many trips of a particular event, such as entering your password, brain activity unrelated to the event in question is reduced. This allows the experimenter to control the cognitive state of the user being reflected in the ERP activity. The CEREBRE protocol was designed for this study to test the hypothesis that controlling the cognitive state of users through specific stimulations could achieve a higher biometric accuracy [60].

A. CEREBRE PROTOCOL

The biometric classification was based on ERP responses to 5 categories of stimulus that should elicit distinct patterns of activation across individuals. Results were compared to biometric accuracy data from a standard eyes-closed EEG acquisition protocol [71] and a pass-thought protocol [10]. The categories of stimulation to evoke ERPs included:

Sine gratings – these were selected as they are known to strongly stimulate the primary visual cortex [9] which varies in its topographical pattern of folds from person to person [8], thus eliciting robust visual potentials over the back of the head [57].

Low-frequency words – these were selected because ERP response to words individuals know the meaning of differs from the response to words individuals do not know. This evidence further indicates that individuals exhibit substantial variation in their knowledge of low-frequency words [39]. Word frequency effect on an ERP is well-characterized as greater negativity for low than high-frequency words beginning around 250ms post-stimulus onset over the back of the head [40, 59]. Individuals response to word-forms was the basis of Ruiz-Blondet et al. [60] previous work with biometrics, which achieved 97% identification accuracy [4]. These words were chosen from the GRE low-frequency word lists and were less than ten letters long.

Images of foods – these images were selected based on the notion that food preference is highly individual. This is accompanied by how the structures in the ventral midbrain exhibit activation profiles, which respond to images of food, vary proportionally to individuals' preferences for those foods [49]. Other examples of ERP responses to food stimuli can be found in [65, 67]. Images were gathered through a pre-experiment study with 44 other people asked to list ten foods they love and ten foods they hate. The most common foods from these lists were chosen.

Celebrity faces – this stimulus was selected based on the observation that celebrities can be polarizing; some celebrities are loved, and others are hated. Structures in the orbitofrontal cortex exhibit activation profiles in response to images of faces that vary proportionally to an individual's judgment of those faces attractiveness [30, 60]. The same pre-experiment study done with food images was conducted with celebrities for selection.

Oddball stimuli – a P300 signal can be detected when someone responds to a rare target stimulus embedded in a sequence of common stimuli. The morphology of the P300 is known to exhibit individual variation. The P300 has been a common basis for the limited work that has been done with ERP biometrics in the past [20]. In this study, oddball stimuli consisted of images from the other four categories, presented in color instead of black and white.

B. METHODS

The study initially consisted of 56 participants with an age range of 18-43 years old, 20.2 years was the mean age. After either failure to follow instructions or equipment malfunction, 50 participants remained for the final database; this is much larger than the reported mean (29 people across ten studies [2]) of participant numbers in other brain biometric studies. No particular screening was used, allowing the study to be as universal as possible [60].

Before the experiment began, participants were asked to select a "pass-thought", after which they were told to think of that "pass-thought" when shown a black key icon during the study. Also, before the experiment, a demonstration on how artifacts like eye-movement during data collection could impact brainwaves was conducted. Research done by Luck [43] has shown how this type of demonstration before a study can improve signal quality.

C. EXPERIMENT

Participants were exposed to 400 images (100 sine, 100 words, 100 food pictures, 100 face pictures, with 300/400 of images in black and white). These 400 images were presented in random order broken into blocks of 100 images. At the beginning and end of each block, participants were prompted to give their pass-thought for roughly three seconds [60]. After the 400 images were shown, 90 randomly selected color food images were presented. One example was the use of a color picture of a hamburger. Participants were asked to respond when they saw that particular hamburger. Finally, towards the end of the experiment, participants were asked to relax by closing their eyes for five minutes. They were not to fall asleep, so this could be used to acquire resting-state EEG readings. In

total, the experiment took approximately 1.5 hours. This included the 30 minutes for EEG electrode placement of 26 active Ag/AgCI electrodes on the scalp, and placement of three electrooculogram (EOG) sensors on the face and one on the right mastoid [60].

ERPs at each electrode were created for every stimulus and included 550 samples, 50 pre-stimuli, and 500 post stimuli. This resulted in a 1100ms ERP. Contrary to what is usually found in ERP literature, ERPs in this study were then filtered with a band-pass of 1-55 Hz for the classification stage rather than below 20 Hz [39, 40, 41]. The value of classifying at a lower frequency is the ability to reduce the impact of muscle activity on the readings. However, this study chose to include higher frequency to leave the cognitive gamma band intact [48].

Classification involved a simple discriminant function based on normalized cross-correlation [60]. Each participant's response to the stimulus were split into two random halves: a challenge half and a reference half. For the 90 responses to colored food, 45 responses were randomly selected and averaged into a reference ERP, and the other 45 were averaged into a challenge ERP. The data from the middle occipital channel was most useful as occipital electrodes capture human primary visual cortex activity [58]. As this study involved visual stimulation, data from this channel was most pertinent. The goal of the classifier was to identify, via cross-correlation, which reference ERP was most similar given a challenge ERP. Each participant's challenge ERP was cross-correlated with their own reference ERP and with the reference ERPs of the other 49 participants.

D. RESULTS

All stimuli, other than resting state, achieved a higher than chance identification accuracy (*Figure 6)*. Also shown is the "field-leading 100% accuracy" from La Rocca et al. [38]. One reason this EEG classifier could have performed poorly here is that no feature extraction was undertaken. This choice was made to have a more direct comparison between the analytic techniques applied to the EEG and ERP. Also, the five primary stimuli were each given 30 trials in both challenge and reference ERPs, while the hamburger and pass-thought classifiers only included five trials. Because of this discrepancy, it is not valid to make direct comparisons between these accuracy results. The best results came from the combination of all six stimuli using data from all 30 nodes. Although this could achieve 100% accuracy, it is a much more in-depth and time-consuming process. Results indicate that all single stimulus, single-channel ERP classifiers were more accurate than pass-thoughts. When multiple channels and stimuli were allowed, accuracy was able to reach 100% which supports the general hypothesis that ERPs might provide accurate biometric results. One reason ERP biometrics could be especially useful is in its ability to connect to functionally distinct brain networks, providing identifying information about a user. By combining a multitude of stimuli with a large number of nodes, using the brains ERPs as a biometric has been proven not only possible but capable of high levels of accuracy [60].

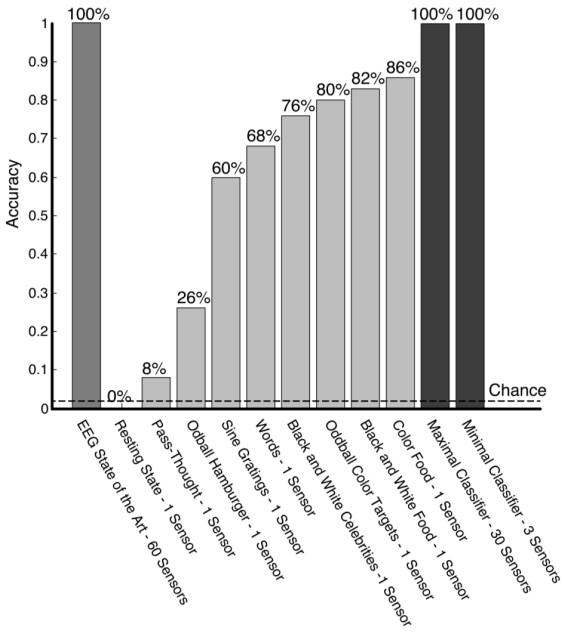

Figure 6: From Ruiz-Blondet et al. [60]

VI. CONTINUOUS AUTHENTICATION

What is uncommon about brainwaves is the possibility of continuous authentication as a new behavioral biometric. Conventional authentication methods that most industries use are static. This

would include passwords, PINs, fingerprint, and iris scanning. Although these methods may have an advantage of being quick and easy to implement, they cannot offer a secure and continuous connection to a system. They do not require users to constantly re-authenticate themselves for continued access. This means systems implementing these security protocols are vulnerable to an attack if someone were to take control of the device once it had been unlocked. One-time authentication may be appropriate for systems where the security requirement is low such as the average person's phone; there could be valuable and personal information on the device, but nowhere near the more valuable data that could be found on a government system. It is likely the place more intense security measures would be required, would be the first to push for adoption of more resilient measures.

The basis of continuous authentication, affirming human identity in real-time, relies on repeated user verification on a loop throughout the session. The system must be able to decide "certainty" at any point in time [3]. Authenticating the user once at the initial log-in stage and once during the session is not enough to assure the user's presence and identity. The advantage of behavioral biometric security is both a safety and convenience factor. Because these attributes are inherent to the individual, they are more natural sources of data. Natural human data sources are the most promising for passive continuous authentication, a method that wouldn't cause authentication to interfere with the user's regular usage. Brainwave metrics could be read on a continuous basis without requiring the user to take additional action to authenticate, a substantial advantage no other system has yet to offer.

One research study that looks into continuous authentication was conducted by Kumar et al. [33]. This work investigated the usefulness of four One-Class Classifiers OCC (elliptic envelope, isolation forest, local outliers factor, and one-class support vector machines) and their fusion. The implementation of a continuous system generally involves use of a sliding window [34, 35, 36]. Authentication decisions are given based on either patterns captured in the current window, or patterns captured in the last few windows. Kumar et al. [33] applied this specifically looking at gait biometrics and phone movement patterns. The findings suggested that it is possible to build a behavior-based biometric continuous authentication system by implementing OCC and their fusion, though no accuracy results were shared [33].

At this stage in brainwave biometrics, no studies have been found that specifically test the validity of continually authenticating via brainwaves. However, research by Maruoka et al. [46] evaluated the possibility of using evoked potentials from auditory stimulation. The use of auditory stimuli does not disturb the user as do formally presented stimuli for other ERP studies [60]. The five participants in this study wore a brainwave sensor by Emotive Cop., were placed in a silent room, and asked to close their eyes and not move their bodies during the experiment. This environment was very controlled, thus attempting to eliminate artifacts.

The stimulus presented was controlled by music-player software and brainwave measurement was controlled by software produced by Emotive Cop. Results from this study showed that evoked potentials from supersonic sounds lead to an increase of the spectrum in the Alpha band at the electrodes on the back of the head [46]. It has also been discovered that the spectrum in the Beta band increased when sounds of favorite tempos are presented [6], which offers the notion that auditory stimulation can provide useful potentials. Thus, there is indication that both audible and inaudible sounds could be a metric continuously presented to a user for verification [46].

VII. ETHICS

More so now than at any point in history is the connectivity and integration of "man and machine" so prevalent in new technology. People store highly personal details on their computers, open phones with the touch of a finger, and rely on implanted biomedical devices to keep them alive. What some refer to as the "connective turn" has created a new mass public where frequent access to machines is required [26, 27]. It is here that the basics of personal identity and privacy become tangled with the expansion of technology and the need to interact, retrieve, and contribute digital content. The social, biological, and technological spheres of society come together in the implementation of biometrics, as human attributes can be reduced to sets of data some argue is a "naïve over-simplification of the uniqueness that characterizes humanity" [54]. Millions of fingerprints have been collected in the United States, Europe, and elsewhere over the years

for use in forensic identification [73]. These biometric measurements have been digitized to form growing interconnected databases that allow quick online searches for the identification of someone. Databases containing this personal information are increasingly interoperating, allowing the sharing of this data among different organizations and across countries [64]. Although this accessibility may have the advantage of convenience, there are ethical concerns associated with the storage and subsequent use of personal and identifiable biometric data. In this regard, certain aspects of the human body are being transformed into a digital representation for consumption by multiple organizations and people. Some would argue that the continued overlap between biology and technology has redefined the human body in terms of information [73]. The points on someone's fingertips are numbers put into a government database for possible authentication later, ECG measurements are shown in a medical file, and even DNA samples are available at fertility clinics. Vital biological information is being shared among the government and corporations in a way not too different than mathematical or financial information is shared.

Often, the integration of the body with security measures involves only superficial contact such as a fingerprint or hand to a scanner. Everything beyond the touching and procurement of the metric to create a digital representation—biometric templates, medical scans, digital images—can be seen as sensitive, personal information [73]. What must be decided is whether the body part itself is only subject to protection, or if the information retrieved from the body should also be given the same privacy rights. It is in this integration of biology and technology that the body itself and information from the body must be distinguished as biometrics further evolve.

The concept of ethics is influenced by law, policy, and cultural norms [64]. It involves balancing competing interests such as advancement of research efforts versus national security concerns. One could ask if it is ethical to collect the DNA of every United States citizen if it is to gather more information to thwart a terrorist attack. Does the notion of "greater good" outweigh physical intrusions from DNA and other biometric readings? Siew et al. [64] discuss five main ethical principles concerning behavioral biometrics:

Privacy – Regarding biometric information, it protects the right for information to not be collected or distributed without informed consent. This can be a challenge when data is frequently shared with third party institutions for evaluation. However, biometric technologies are evolving to the point where interoperability standards could pose ethical dilemmas.

Confidentiality – The sharing of information is often of benefit in the scientific community, however, potential threats to the confidentiality of data being distributed online is a problem for sensitive biometrics. It has been argued that it is impossible to achieve absolute confidentiality and constant access to patient information [56]. This could be an issue if a person's biometric data is meant to be stored and assessed across multiple platforms.

Security – Data and system security are two of the main types. Data security relates to the protection of data from accidental or intentional disclosure to unauthorized persons, while system security protects the confidential information thereby protecting the privacy of the individuals who are the subjects of stored information [64].

Property and Ownership – This principle is perhaps the hardest to differentiate when it comes to biometric data. Some would argue that patient medical files or biometric data belongs to the person who collects, compiles, and holds it such as a medical practitioner or software company. Others would say the patients or users are the rightful owners of that information, as they have the access rights because that information came from their body. Regarding biometric data, this raises the question whether the user owns the data used for biometric authentication, or if ownership falls to the person who possesses the biometric [29].

Reliability and Trustworthiness – At the core of biometric applications should be the notion of trust that error and harm will be minimized. Reliability is not guaranteed with biometrics as matching is based on probability. As such, it is possible that certain people will have a more favorable experience using biometrics, and this could render the system more trustworthy for some over others. Standardization of biometric requirements helps with trustworthiness; if the public is more accepting of the system, the trust will increase.

Deliberate misuse most commonly occurs in the context of criminal activity where the information is obtained to be sold or used for theft such

as with identity. Unintentional data leakage is difficult to address, although it violates ethical principles. One example was when medical data from 100 patients was mistakenly emailed to recipients who should not have had that information [69]. This act was unintentional, yet still caused harm. Finally, business practices can lead to the misuse of data if the data is not stored and erased properly. Data could also be shared across business units under the same corporation [64]. The more sensitive biometric data is shared, the more likely it is to end up released or suffer misuse.

VIII. ONGOING CHALLENGES

As the feasibility of brainwave authentication continues to grow, ongoing challenges with the development should be addressed. This section will discuss issues of security (I), impersonation attacks (II), discrimination and failures with biometrics (III), and the leakage of sensitive information that could happen with brainwave authentication (IV).

I. NEUROSECURITY

Security concerns are particularly significant with technology that has access to sensitive personal information such as with medical devices. The caveat of neural devices is that a communication pathway must be established to the nervous system in order allow computer systems access and the ability to process neural computation [28]. It is this accessibility that is both paramount for effective use of the device, and also the feature that offers the biggest area for security risks, specifically concerning privacy. As neural computation involves the behavior and cognition of a person, ethical safeguards taking into account the possible physiological and psychological harm that could occur should be considered early in product design [23].

One example of this emerging risk can be found by Halperin et al. [22]. An experiment was conducted which demonstrated a hacker could wirelessly compromise the privacy and security of a commercial cardiac defibrillator implant [23]. This intrusive act was achieved through surprisingly simple measures with homemade and low-cost equipment. The outcome of this hack was the ability to change or disable the patient's therapies, and induce potentially fatal processes. This is proof that security of bioengineering devices is not only about keeping private information secure, but also about preventing potentially cataclysmic and fatal events.

Some specific security concerns with brainwave authentication include attacking the authentication system via synthetic EEG signals. The adversary could build an EEG model based on historical EEG data from a user [42]. However, due to the complexity of the brain, this threat could be thwarted by building a more robust authentication system leveraging a multimodal approach. Risks associated with BCI devices, such as those used for collecting EEGs, are largely unexplored. BCIs are potentially vulnerable to cyber criminality in a new area known as "neurocrime". This involves the extension of what constitutes a computer-crime to include technologies with a connection to the brain such as neural devices [23].

A specific type of neurocrime referred to as "brain-hacking" aims to gain access to and manipulate neural information and computation [23]. Within this field, there are more requirements, as it can only be performed through a connection with the brain such as with neural implants or BCIs, and leads to the direct access, manipulation, and influence of neural computation. This could be done through the use of an EEG device. With the brain acting as a vital organ maintaining life processes as well as faculties, misuse of neural devices for criminal purposes not only threatens physical security and possibly access to systems, it could also influence the user's behavior and later their self-identification as a person [23]. Neurocrime, however, does not necessarily require direct access to the brain and brain information. Neurocriminal activities most likely impact the brain indirectly.

Brain-hacking can be executed at multiple stages of authentication or use of a neural device. The main four junctions where this could occur are input manipulation at the start, measurement, decoding and classification, and feedback [23]. Beginning with input manipulation, this occurs when the hacker attacks the user at the moment when input to the system is being provided. An alteration of the stimuli presented to the user could offer an advantage to the hacker by preselecting target stimulants to elicit a specific response. One study to test the feasibility of this attack was Martinovic et al. [45]. Given six separate classes of stimuli—PIN code digits, bank related photos, month names,

debit card digits, locations, and faces—one target stimulus for each class was placed in a randomly permuted sequence of non-target stimuli. An example of this would be during the "bank experiment" when a picture of an ATM from the user's bank was the target stimulus. Pictures of ATMs from other banks would serve as the non-target stimuli. Detection of a P300 signal in response to private information, such as recognition of a user's particular ATM, could be used to indicate personal information. These results show that input-manipulation could be used to attack the private information of a user.

Regarding measurement manipulation, brain-hacking could occur to generate output different than those expected through regular processing [23]. Some reasons an attack may happen in this manner could be to crack the BCI's raw data, disrupt BCI functionality, or hijack the device itself. As explained by Conner [11], a hacker named Cody Brocious was able to crack the encryption on the EPOC Emotiv BCI, allowing someone to read encrypted data directly from the headset. Despite this intrusion potential, it only allows the pulling of raw data from the device, how the signals and sensors correspond to each stream of data must still be deduced. Attacks during this measurement stage could allow the hacker to alter the measuring process, perhaps adding noise, opening the door to sabotage or delay of BCI application functionality.

Similar to the phase above, brain-hacking at the decoding and classification level is also aimed at creating outputs different than those intended by the user. As discussed by Haselager et al. [23], an adversary could achieve this by adding noise or altering the machine learning component used for classification. A noise-adding hack has the advantage of being relatively easy to perform and less likely to be detected. This could bode well for an attacker who hopes to remain unnoticed. In contrast, if an adversary wishes to gain more control over a BCI device or application, overriding the signal sent to the output device could prove a more dangerous method. A successful hijacking attempt could involve the system being given different commands than those intended, resulting in control over the BCI application [23]. One use for this attack could include the blocking of an authentication attempt by a user. The inability to gain access to a device could be just as serious as the inability to control it.

Finally, feedback manipulation is another stage in which brain-hacking could happen. At the end of each cycle, feedback is perceived by the user. A hack in this phase would revolve around the alteration of user perceptions. The goal of an attack would be to induce a particular cognitive state or action, which the user did not authorize. This could result in criminal activities such as fraud, identity theft, and physical or psychological harm [23].

One common threat model surrounds a spoofing attack; an adversary could use some manufactured biometric data to gain access [62]. In the threat model by Sadeghi et al. [62], there are three components to an attack: adversary's knowledge, adversary's capability, and the adversary's goal.

i. Knowledge – One example would be a grey-box attack where it is assumed an adversary has access to some biometric samples with the subject's data. In this scenario, it is also given that the feature type and extractor are known, such as brainwaves, but the classifier is unknown.
ii. Capability – The main capability of an adversary would be to present raw input data into the system. In the case of brainwaves, the adversary would have to deduce a single feature and convert that into raw EEG signals. In this sense, a brute-force attack would likely take place as it would require guessing all possible combinations until a positive response was received from the system. Because brainwaves are unique and highly complex based on the stimuli, this task would be difficult, and perhaps the adversary's greatest hurdle to intrusion.
iii. Goal – The objective is to obtain a viable signal such that it can be correctly classified in the target subject's class, resulting in authentication. Within this category, the adversary has two choices in how to pursue—replay attack and manufacturing data. A replay attack involves reusing snooped data, which can be blocked by applying a similarity check between historical signal data and new data. This ensures that the data is not the same as the stored data, implying it was stolen and indicating a possible threat. Manufacturing input data would require information regarding the feature extraction algorithm in addition to the range and dimensions of data features. The adversary could begin by guessing feature vectors and

regenerating raw input through reverse feature extraction algorithms [62].

At the current level of sophistication and prevalence of brain-hacking, the benefits of BCI development are far greater than the risks that could manifest relating to neurocrime and brain-hacking. Mild-forms of brain-hacking have been proven feasible in laboratory settings, but no real-world examples have appeared at the severity discussed in research. The level of accuracy and speed at which someone would have to decode brain signals is far from what can be done currently with computer code.

II. IMPERSONATION ATTACKS

As mentioned in the prior paragraph, a major security concern with any authentication system is the likelihood that someone could impersonate a user to gain access. With traditional biometrics such as fingerprints, this is relatively easy to achieve with the right image and data on the subject. However, this becomes considerably harder when the data used for authentication resides in the consciousness of the user. A study completed by Johnson et al. [31] tests whether brainwaves are vulnerable to impersonation during authentication.

This research was an extension of prior work conducted by Chuang et al. [10] in which brainwaves were used to create an authentication system with 99% accuracy. The original study involved 15 subjects performing seven mental tasks, during which brainwave signals were collected ten times per subject per task. The seven mental tasks used in the original study were also used to test for imposters in this study. Below are the descriptions and instructions for each mental task completed by the subjects as described by Johnson et al. [31].

i. Breathing – "Close your eyes and focus on your breathing for 10 seconds."
ii. Simulated Finger Movement – "Imagine in your mind that you are moving your right index finger up and down in sync with your breathing, without actually moving your finger, for 10 seconds."
iii. Sports – "Select a specific repetitive motion from a sport of your choosing. Imagine moving your body muscles to perform this motion, for 10 seconds."
iv. Song/Passage Recitation – "Imagine that you are singing a song or reciting a passage for 10 seconds without making any noise."
v. Eye and Audio Tone – "Close your eyes and listen for an audio tone. After 5 seconds, the tone will play; upon hearing the tone, open your eyes and stare at the dot on the piece of paper in front of you for an additional 5 seconds."
vi. Object Counting – "Choose one of four colors – red, green, blue, or yellow. You will be shown on a computer screen a sequence of six images. Each image contains a 5x6 grid of colored boxes. As each grid appears, count, silently in your mind, the number of boxes corresponding to your chosen color. A new grid will appear after each 5 seconds. This will continue six rounds for a total of 30 seconds."
vii. Pass-thought – "Choose your own pass-thought. A pass-thought is like a password; however, instead of choosing a sequence of letters and numbers, one chooses a mental thought. When instructed to begin, focus on your pass-thought for 10 seconds."

One question addressed in this research was whether knowledge of a subject's chosen task impacts the success of an impersonation attack [31]. The acceptance rate for imposters was approximately 4.5% with four of the subjects' experiences false acceptance rates less than 1.2%. One of the most difficult tasks to impersonate was the "song task", where the original subject had selected the "Serbian National Anthem" [31]. The imposters themselves had extreme difficulty impersonating this thought on their own, due to the language barrier and unfamiliarity. It was discovered that, in general, the imposter authentication success rate is low. Knowing the subject's task, or task secret, only provided a small improvement over thinking about another topic entirely. This shows, that even if an attacker knows what to think about during authentication to impersonate a user, it is unlikely the brainwave signals will match enough to offer authentication.

III. DISCRIMINATION AND FAILURES

In the United States, as of July 1st, 2014, the number of people who were 65 and older was approximately 46.2 million which accounts for 14.5% of the total population [72]. It is also estimated that by 2060 that number will be nearly one in four US residents at around 98.2 million people [72]. This increase in older adults brings about the question of inclusion as biometric technologies proliferate the industry. The common notion is that new technology is only for the younger generation, as it is them who tend to adopt products earlier and integrate them into their lives faster. Older adults, particularly those reaching ages over 65 in the 2010s, are facing the rapid integration of technology. Where banks used to be only in brick-and-mortar stores, now operate through web portals or phone apps. Although these products are made readily available to all sectors of the population, it is often that older adults are excluded from the mass adoptability that benefits most technology. As biometric authentication systems become more prolific, and as they are integrated into a wider range of activities such as banking, benefits, and goods purchasing, it is essential biometrics are both convenient and reliable for all people. If biometrics fail to identify older people efficiently, the problematic minority concerning technology adopters will rapidly become the majority, and new forms of biometric authentication such as brainwaves will fail as a widespread tool [53].

Unlike passwords and PINs, where the alphabet and numbers will never change, no biometric feature is fully permanent over time. Almost all features show significant deterioration as people age, and those that are most permanent such as DNA are difficult to collect. A consequence of this relative instability is the deterioration of quality in each metric, particularly with older adults who could be prone to failure-to-enroll biases in biometric systems [53]. One example can be found in the Unique ID program in India, which aimed to provide a national biometric system that could identify the members of its 1.1 billion inhabitants. Ultimately, it had difficulty enrolling those above the age of 65 [53]. Three modalities were proposed—face, fingerprint, and iris—and problems with each modality emerged pertaining to deterioration with age.

i. Faces show clear change over time as the collagen in the body decreases leading to wrinkling, sagging, skin elasticity, and changes in skull and jaw dimensions.
ii. The quality of fingerprint ridge structures lessens with age as the physical definition is lost. Lower collagen levels create suboptimal contact with the sensor which can lead to an unclear reading of the fingerprint.
iii. It used to be believed that the iris was an extremely permanent feature as it is an internal organ of the eye [12]. This has changed, however, as conditions such as cataracts and glaucoma could alter iris appearance [37].

Where authentication systems falter is in the time between when the original template is created and when someone attempts to be identified later. If there has been a significant amount of time between the generation of the two templates, an individual's biometric feature could have changed enough that the score fails to meet the system's threshold [53]. This is known as template aging, and it does not only concern older adults in isolation. Template aging can impact anyone for whom there has been a significant amount of time since their enrollment in a system. This time-lapse, although problematic for anyone, can be particularly detrimental for the older population as significant alterations in features are more likely to occur later in life. This is mostly due to the natural aging process and higher likelihood medical conditions could play a role [53]. Some recommended solutions to template aging could include template updates and exploiting age-invariant features. With the first example, this would involve updating templates and re-enrolling individuals, an extensive and costly endeavor. On the other hand, trying to find biometric features that are immutable is an equally difficult task. Some parts of the face do change less over time, but all parts of the body experience change over a lifetime and thus weaken the usability of static biometrics [53]. As suggested, a way to combat this inevitable physical change could be to focus on more intuitive behavioral metrics such as brainwaves. Although the brain does evolve, the way people inherently process information is relatively stagnant. As mentioned in section VI on continuous authentication, the brain is uniquely positioned to act as an ever flowing and evolving authentication metric. Significant advances in machine learning and artificial intelligence could create the possibility of a template that evolves as the user does. As

the brain experiences more, a better fitting model of how an individual's brainwaves present can be created. Through repeated use with brainwave authentication, templates could grow to fit the user, eliminating the need to handle metrics that become outdated.

IV. SENSITIVE INFORMATION REVEALED

Another ethical and security dilemma to consider is whether the use of a brainwave authentication reveals highly personal and sensitive information about the user. The main goal of designing an authentication system is to maximize the accuracy. This does not raise many problems when using conventional methods, or even with most static biometric measures. It is true that fingerprints reveal biological information about the user; however, it does not reveal sensitive personal information as behavioral biometrics do. Having the fingerprint of an individual doesn't divulge medical conditions or behavioral tendencies. This is not the case with brainwaves since brainwaves encode a multitude of other potentially sensitive information about the user. Multiple variables are used creating an authentication device including the features to build user templates, signal frequency ranges for extraction, and the location on the scalp for electrode placement. As suggested by Matovu et al. [47], a "single-pronged, privacy-agnostic approach" focused only on accuracy could have severe privacy implications. In the majority of studies done on brainwave authentication, researcher's primary agenda is to lower system error rates. Certain design attributes in the authentication system might be more prone to potential leakage of personal information. If a system with the lowest authentication error rates also divulges significantly higher amounts of personal data, it begs the question whether the trade-off is practical and ethical. The research conducted by Matovu et al. [47] hypothesizes, with the assumption that all system variables have been optimized for authentication accuracy, whether a malicious entity could exploit the biometric templates to infer non-authentication-centric information regarding the user. Other questions considered include if inferences are possible, whether particular template designs would be more vulnerable than others and if a more robust collection of sensitive information could be gleaned—emotions, medical conditions, and learning abilities.

Matovu et al. [47] looks specifically at the behavior of substance abuse, the condition of being an alcoholic. The revelation of such information could have not only cyber security implications but legal ones as well. The threat model used in this study was based on the assumption that an attacker would have access to a database of EEG authentication templates, thus eliminating the initial question of determining what metric and templates are used. In this case, the attacker must have had inside knowledge about the template formulation to exploit the system fully. Because this study is evaluating the personal information about a subject, it is not as concerned with the manner in which an adversary acquires the tools to exploit the system. The dataset used was collected by Neurodynamics Laboratory, SUNY Downstate Medical Center, of which 50 subjects were chosen—25 from each of the alcoholic and control groups. All subjects were detoxed 30 days prior to data collection, and each provided 30 samples for the study. Two templates were created specifying different electrode placement of the scalp.

i. Template 1 – Six electrodes were placed on the scalp with each electrode giving a total of six features. After computing the spectral density from the signals of each electrode, only the data from alpha and beta ranges was retained, where three features were computed: entropy, mean, and standard deviation.
ii. Template 2 – This template only used one electrode, the Front Polar, placed near the frontal lobe. Again, only data from alpha and beta ranges was retained once the power spectral density was computed for the electrode.

These two templates gave mean Half Total Error Rate (HTER) of between 0.155 and 0.264 with HTER calculated as $HTER = \frac{FMR+FNMR}{2}$ [44]. Although these error rates are far outside those for a system ready for deployment, they are not too far from those previously reported in the literature [10, 44].

Through the use of a mutual information metric, the dependency between a user's template and alcohol use behavior can be understood. Mutual information can detect non-linear relationships, thus

enabling the researcher to get a rigorous account of how an EEG biometric template could reveal information about a user's behavior regarding alcohol abuse. In this study, mutual information between the biometric class labels and biometric features, and the mutual information between the same biometric features and the alcohol use class labels (if a user is alcoholic or not) were analyzed.

From the first angle, the evaluation gives insights into the intensity in which the features reduce uncertainty about the user's identity—referred to as the MI_{auth} setting. The second approach gives information about how strongly the features reduce uncertainty about the user's alcohol usage behavior—referred to as the MI_{alco} setting. In the context of building an accurate and private authentication system, the goal would be to have high amounts of mutual information from the MI_{auth} setting, while also maintaining less mutual information from the MI_{alco} setting. If the MI_{alco} setting exhibits higher mutual information, thus a stronger dependency, then it is probable the system's high authentication accuracy comes at the cost of the leakage of user personal information [47]. The conclusion reached by the researchers conducting this study [47] found that for almost 25% of the population in the study, the authentication template divulged a significantly higher amount of information about their alcohol use behavior than it did for the primary authentication goal.

Alcoholism is just one behavioral element that could be inferred from brainwave analysis. By making variable changes in the locations of EEG electrodes and feature extraction, it is possible that other behaviors could be gleaned. However, it was also found that in changing some of the above-mentioned variables, the security of a template could be increased while only causing a slight reduction in the mean authenticity accuracy. This proves that it might be possible to find an optimal solution of electrode placement and feature extraction that minimizes information leakage while maintaining a reliable level of authentication accuracy. Despite that fact that some personal information can be gleaned through brainwave authentication, the newness of this development inspires the chance that in the future a more secure solution could be discovered.

IX. FUTURE PROSPECTS

Acceptability can be one of the most difficult hurdles when introducing a new authentication system. A research study was conducted by Halevi et al. [21] to test how comfortable people felt giving their biometric data to a website. The experiment included 100 participants with 73% of them under 24 years old. As this demographic is more likely to try new technology, biometric acceptability within this category is necessary for the success of an authentication system. When participants were shown two mock websites, the familiar "Amazon" and a newly created "Amazin", they were asked if they would be willing to share their fingerprints for a $50 discount for each site. Participants were also asked whether they had been victim to a computer hack in the past such as identity theft, malware, and viruses. It was discovered that people who had experienced some computer hack were much less likely to share their biometrics. Only 28% of participants who had experienced a virus attack would provide their fingerprints. This metric is not surprising, as the willingness to share personal information often depends on whether a person has had that information compromised before. What is more interesting is that only 56% of participants who did not experience an attack would provide fingerprints [21]. Despite not having experienced any malicious activity, people are still suspicious of giving out their biometric data, even when offered monetary gain. Considering this study was done with the more common fingerprint biometric, the likelihood users would be willing to share brainwave biometrics is much lower, especially if personal information can be deduced from this collection.

A biometric authentication device will undoubtedly be met with skeptical users, particularly when the possibility of a computer hack is evermore present. Although biometric authentication has not reached extremely high acceptability, the growth of the industry will be a catalyst for new methods and higher use. The size of the biometrics market in the US is growing (*Figure 7)*, and expected to increase rapidly over the next decade. The more biometric devices permeate through society, the more likely acceptability will increase, opening the door to new forms of biometrics, such as brainwave authentication. Coupled with the commerciality of EEG devices and the societal need for security, brainwave

authentication is the next logical step. Once brainwave authentication has crossed the chasm to be a moderately accepted form of security, the next phase will see an expansion in research of continuous authentication methods. No longer will login-time security measures be enough for the technology-driven world. The unique conscious enabled data the brain provides can offer the next level of security. Studies in this area are limited and extremely new, but as research in the brain, biometrics, machine learning, and artificial intelligence progress, continuous authentication via brainwaves could come to fruition.

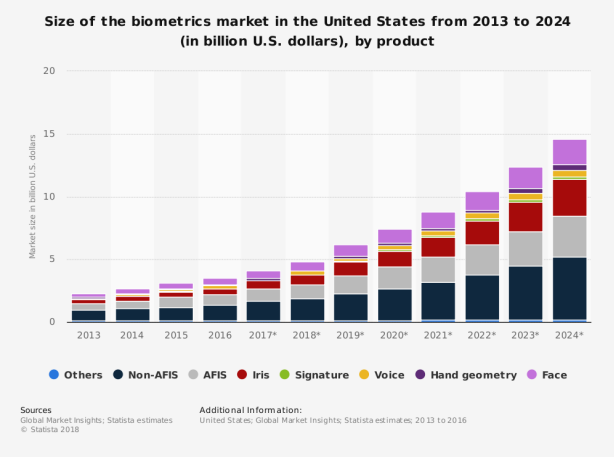

Figure 7: From Statista [66]

X. CONCLUSION

This paper discussed the possibilities of using brainwaves as a behavioral biometric for user authentication. Through analysis of research studies, it has been shown that brainwave authentication can achieve accurate results above 96%, especially when implementing a multi-metric approach. The brain can offer a unique metric capable of standing as an authentication method, and as further progress is made in this research, it is possible continuous authentication methods could be introduced. The highly complex and personal data emitted by the brain, however, raises security concerns that cannot be ignored when pursuing brainwave authentication. The balance of accuracy and privacy will be paramount in this endeavor.

XI. ACKNOWLEDGEMENT

This project was supported by the Honors Undergraduate Research Fund administered by Honors Carolina.

REFERENCES

[1] M. K. Abdullah, K. S. Subari, J. L. C. Loong, and N. N. Ahmad, "Analysis of the EEG signal for a practical biometric system," *World Acad. Sci., Eng. Technol.*, vol. 68, no. 44, pp. 1123–1127, 2010.

[2] A. Almehmadi and K. El-Khatib, "The state of the art in electroen- cephalogram and access control," in *Proc. 3rd Int. Conf. Commun. Inf. Technol. (ICCIT)*, 2013, pp. 49–54.

[3] A. Altinok and M. Turk, "Temporal integration for continuous multi- modal biometrics," in *Proceedings of the Workshop on Multimodal User Authentication*. Citeseer, 2003.

[4] B.C. Armstrong, M. V. Ruiz-Blondet, N. Khalifian, K. J. Kurtz, Z. Jin, and S. Laszlo, "Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics," *Neurocomputing*, vol. 166, pp. 59–67, Oct. 2015.

[5] M. K. Bashar, I. Chiaki and H. Yoshida, "Human identification from brain EEG signals using advanced machine learning method EEG-based biometrics," 2016 IEEE EMBS Conference on Biomedical Engineering and Sciences (IECBES), Kuala Lumpur, 2016, pp. 475-479.
doi: 10.1109/IECBES.2016.7843496

[6] A. K. R. Bauer, Kreutz and C. S. Herrmann, "Individual Musical Tempo Preference Correlates with EEG Beta Rhythm", Psychophysiology, Vol. 52, No. 4, pp. 600-604, 2015.

[7] M. Blondet, S. Laszlo, and Z. Jin. (2015). Assessment of Permanence of Non-volitional EEG Brainwaves as a Biometric. 2015 IEEE International Conference on Identity, Security and Behavior Analysis, ISBA 2015. 10.1109/ISBA.2015.7126359.

[8] H. Bridge, S. Clare, M. Jenkinson, P. Jezzard, A. J. Parker, and P. M. Matthews, "Independent anatomical and functional measures of the V1/V2 boundary in human visual cortex," *J. Vis.*, vol. 5, no. 2, pp. 93–102, 2005.

[9] M. Carandini, D. J. Heeger, and J. A. Movshon, "Linearity and normalization in simple cells of the macaque primary visual cortex," *J. Neurosci.*, vol. 17, no. 21, pp. 8621–8644, 1997.

[10] J. Chuang, H. Nguyen, C. Wang, and B. Johnson, "I think, therefore i am: Usability and security of authentication using brainwaves," in *Financial Cryptography and Data Security*. Berlin, Germany: Springer, 2013, pp. 1–16.

[11] M. Conner. (2010). Hacking the brain: Brain-to-computer interface hardware moves from the realm of research. EDN, 55(22), pp. 30–35.

[12] J. Daugman, "How iris recognition works", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14. No. 1, 2004, pp. 21-30.

[13] R. Dhamija and A. Perrig. Déjà Vu: A User Study Using Images for Authentication. In 9th USENIX Security Symposium, 2000.

[14] M. Doppelmayr, W. Klimesch, T. Pachinger, and B. Ripper. Individual Differences in Brain Dynamics: Important Implications for the Calculation of Event-Related Brain Power, 1998.

[15] T. Elbert, C. Pantev, C. Wienbruch, B. Rockstroh, and E. Taub. Increased Cortical Representation of the Fingers of the Left Hand in String Players. Science, 270:305–307, 1995.

[16] R. Fazel-Rezai, B. Z. Allison, C. Guger, E. W. Sellers, S. C. Kleih, and A. Ku¨bler. (2012). P300 brain computer interface: Current challenges and emerging trends. Frontiers in Neuroengineering, 5(14), 14.

[17] K. Fladby. (2008). Brain Wave Based Authentication (Master's Thesis). Gjøvik University College. Retrieved from

https://brage.bibsys.no/xmlui/bitstream/handle/11250/143821/Kennet_Fladby_Brain_Wave_Based_Authentication_Final.pdf?sequence=1

[18] D. Frank, J. Mabrey and K. Yoshigoe, "Personalizable neurological user authentication framework," 2017 International Conference on Computing, Networking and Communications (ICNC), Santa Clara, CA, 2017, pp. 932-936. doi: 10.1109/ICCNC.2017.7876258

[19] C. Freudenrich and R. Boyd. (2001, June 6). How Your Brain Works. *Howstuffworks*. Retrieved September 13, 2017, from https://science.howstuffworks.com/life/inside-the-mind/human-brain/brain1.htm

[20] C. N. Gupta, R. Palaniappan, and R. Paramesran, "Exploiting the P300 paradigm for cognitive biometrics," *Int. J. Cognit. Biometrics*, vol. 1, no. 1, pp. 26–38, 2012.

[21] T. Halevi, T. K. Kuppusamy, M. Caiazzo and N. Memon, "Investigating users' readiness to trade-off biometric fingerprint data," *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015)*, Hong Kong, 2015, pp. 1-8. doi: 10.1109/ISBA.2015.7126366

[22] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, et al. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In IEEE symposium on security and privacy, 2008, SP 2008.

[23] P. Haselager, and M. Ienca. (2016). Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity. Springer. doi:10.1007/s10676-016-9398-9

[24] C. He and J. Wang, "An Independent Component Analysis (ICA) Based Approach for EEG Person Authentication," 2009 3rd International Conference on Bioinformatics and Biomedical Engineering, Beijing, 2009, pp. 1-4. doi: 10.1109/ICBBE.2009.5162328

[25] B. D. Hond. (2015, May 19). Your brain's unique response to words can reveal your identity. *New Scientist*. Retrieved November 20, 2017, from https://www.newscientist.com/article/dn27555-your-brains-unique-response-to-words-can-reveal-your-identity/

[26] A. Hoskins. (2011) 7/7 and Connective Memory: Interactional trajectories of remembering in post-scarcity culture. Memory Studies. 4(3), pp. 269-280, 2011.

[27] A. Hoskins, (2012) Media and Memory. Cambridge MA: MIT Press.

[28] M. Ienca. (2015). Neuroprivacy, neurosecurity and brain-hacking: Emerging issues in neural engineering. Bioethica Forum. Volume 8. pp. 51-53.

[29] ICITS. InterNational Committee for Information Technology Standards. (2007). Study Report on Biometrics in E-Authentication. Retrieved from http://www.incits.org/tc_home/m1htm/m1070185rev.pdf

[30] A. Ishai, "Sex, beauty and the orbitofrontal cortex," *Int. J. Psychophysiol.*, vol. 63, no. 2, pp. 181–185, 2007.

[31] B. Johnson, T. Maillart, and J. Chuang. (2014). My thoughts are not your thoughts. UbiComp 2014 - Adjunct Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing. 1329-1338. 10.1145/2638728.2641710.

[32] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *Advances in neural information processing systems*, pp. 1097–1105, 2012.

[33] R. Kumar, P. P. Kundu and V. V. Phoha, "Continuous authentication using one-class classifiers and their fusion," *2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)*, Singapore, Singapore, 2018, pp. 1-8. doi: 10.1109/ISBA.2018.8311467

[34] R. Kumar, V. V. Phoha, and A. Serwadda. Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns. In IEEE (BTAS), pages 1–8, Sept 2016. doi: 10.1109/BTAS.2016.7791164.

[35] R. Kumar, V. V. Phoha, and A. Jain. Treadmill attack on gait-based authentication systems. In 2015 IEEE (BTAS-2015).

[36] R. Kumar, VV. Phoha, and R. Raina. Authenticating users through their arm movement patterns. CoRR, abs/1603.02211, 2016. URL http://arxiv.org/abs/ 1603.02211.

[37] A. Lanitis, "A survey of the effects of aging on biometric identity verification", International Journal of Biometrics, vol. 2, no. 1, 2010, pp. 34-52.

[38] D. La Rocca *et al.*, "Human brain distinctiveness based on EEG spectral coherence connectivity," *IEEE Trans. Biomed. Eng.*, vol. 61, no. 9, pp. 2406–2412, Sep. 2014.

[39] S. Laszlo and K. D. Federmeier, "Better the DVL you know: Acronyms reveal the contribution of familiarity to single-word reading," *Psychol. Sci.*, vol. 18, no. 2, pp. 122–126, 2007.

[40] S. Laszlo and K. D. Federmeier, "Never seem to find the time: Evaluating the physiological time course of visual word recognition with regression analysis of single-item event-related potentials," *Lang., Cognit. Neurosci.*, vol. 29, no. 5, pp. 642–661, 2014.

[41] S. Laszlo and K. D. Federmeier, "The n400 as a snapshot of interactive processing: Evidence from regression analyses of orthographic neighbor and lexical associate effects," *Psychophysiology*, vol. 48, no. 2, pp. 176–186, 2011.

[42] Q. Li, D. Ding and M. Conti, "Brain-Computer Interface applications: Security and privacy challenges," 2015 IEEE Conference on Communications and Network Security (CNS), Florence, 2015, pp. 663-666. doi: 10.1109/CNS.2015.7346884

[43] S. J. Luck, *An Introduction to the Event-Related Potential Technique*. Cambridge, MA, USA: MIT Press, 2005.

[44] S. Marcel and J. Millan. (2007). Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation. IEEE transactions on pattern analysis and machine intelligence. 29. 743-52. 10.1109/TPAMI.2007.1012.

[45] I. Martinovic, D. Davies, M. Frank, D. Perito, T. Ros, and D. Song. 2012. On the feasibility of side-channel attacks with brain-computer interfaces. In Proceedings of the 21st USENIX conference on Security symposium (Security'12). USENIX Association, Berkeley, CA, USA, pp. 34-34.

[46] T. Maruoka, K. Kambe, H. Harada and I. Nakanishi, "A study on evoked potential by inaudible auditory stimulation toward continuous biometric authentication," *TENCON 2017 - 2017 IEEE Region 10 Conference*, Penang, 2017, pp. 1171-1174. doi: 10.1109/TENCON.2017.8228034

[47] R. Matovu and A. Serwadda, "Your substance abuse disorder is an open secret! Gleaning sensitive personal information from templates in an EEG-based authentication system," *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, Niagara Falls, NY, 2016, pp. 1-7. doi: 10.1109/BTAS.2016.7791210

[48] S. D. Muthukumaraswamy and K. D. Singh, "Visual gamma oscillations: The effects of stimulus type, visual field coverage and stimulus motion on MEG and EEG recordings," *NeuroImage*, vol. 69, pp. 223–230, Apr. 2013.

[49] J. O'Doherty , T. W. Buchanan, B. Seymour, and R. J. Dolan, "Predictive neural coding of reward preference involves dissociable responses in human ventral midbrain and ventral striatum," *Neuron*, vol. 49, no. 1, pp. 157–166, 2006.

[50] R. Palaniappan and D. P. Mandic, "Biometrics from brain electrical activity: A machine learning approach," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 738–742, Apr. 2007.

[51] A. Perrig and D. Song. Hash Visualization: a New Technique to Improve Real-World Security. In International Workshop on Cryptographic Techniques and E-Commerce, pages 131–138, 1999.

[52] M. Pugh, (1977). *The Biological Origin of Human Values*.

[53] P. Rebera and B. Guihen, "Biometrics for an ageing society societal and ethical factors in biometrics and ageing," *2012 BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG)*, Darmstadt, 2012, pp. 1-4.

[54] Renaud, A. Hoskins and R. von Solms, "Biometric identification: Are we ethically ready?," *2015 Information Security for South*

Africa (ISSA), Johannesburg, 2015, pp. 1-8. doi: 10.1109/ISSA.2015.7335051

[55] A. Riera, A. Soria-Frisch, M. Caparrini, C. Grau, and G. Ruffini, "Unobtrusive biometric system based on electroencephalogram analysis," *EURASIP J. Adv. Signal Process.*, no. 1, pp. 1–8, 2008.

[56] D.M Rind, I.S. Kohane, P. Szolovits, C. Safran, H.C. Chueh, and G.O. Barnett.(1997). Maintaining the Confidentiality of Medical Records Shared over the Internet and the World Wide Web. *Annals of Internal Medicine,* 127(2): 138-141

[57] U. Roeber, "Neural processing of orientation differences between the eyes' images," *J. Vis.*, vol. 12, no. 13, p. 20, 2012.

[58] B. Rossion and C. Jacques, "The N170: Understanding the time course of face perception in the human brain," in *The Oxford Handbook of Event-Related Potential Components*. Philadelphia, PA, USA: Elsevier, 2011.

[59] M.D. Rugg, "Event-related brain potentials dissociate repetition effects of high- and low-frequency words," *Memory Cognit.*, vol. 18, no. 4, pp. 367–379, 1990.

[60] M.V. Ruiz-Blondet, Z. Jin, and S. Laszlo, "CEREBRE: A novel method for very high accuracy event-related potential biometric identification," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1618–1629, 2016.

[61] K. Sadeghi, A. Banerjee, J. Sohankar and S. K. S. Gupta, "Geometrical Analysis of Machine Learning Security in Biometric Authentication Systems," *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Cancun, 2017, pp. 309-314. doi: 10.1109/ICMLA.2017.0-142

[62] K. Sadeghi, J. Sohankar, A. Banerjee, and S. Gupta. A novel spoofing attack against electroencephalogram-based security systems. In *Advanced and Trusted Computing (ATC), The 14th IEEE Conference on*, 2017.

[63] R. Saracco. (2017, March 20). What is the computational power of our brain? Retrieved November 8, 2017, from https://www.eitdigital.eu/news-events/blog/article/what-is-the-computational-power-of-our-brain

[64] S. T. Siew *et al*., "Ethical implications of digitised medical and biometric data," *eChallenges e-2010 Conference*, Warsaw, 2010, pp. 1-9.

[65] D. M. Small *et al.*, "Human cortical gustatory areas: A review of functional neuroimaging data," *NeuroReport*, vol. 10, no. 1, pp. 7–14, 1999.

[66] Statista. (n.d.). Size of the biometrics market in the United States from 2013 to 2024 (in billion U.S. dollars), by product. In *Statista - The Statistics Portal*. Retrieved March 16, 2018, from https://www-statista-com.libproxy.lib.unc.edu/statistics/761213/biometrics-market-size-by-product-in-us/.

[67] J. Stockburger and R. Schmälzle, T. Flaisch, F. Bublatzky, and H. T. Schupp, "The impact of hunger on food cue processing: An event-related brain potential study," *NeuroImage*, vol. 47, no. 4, pp. 1819–1829, 2009.

[68] P. Tangkraingkij. (2017). An Appropriate Number of Neurons in a Hidden Layer for Personal Authentication Using Delta Brainwave Signals. 10.1109/ICCRE.2017.7935076.

[69] The Register. (2009). "NHS Direct wrongly emailed patients' data". Retrieved from http://www.theregister.co.uk/2009/07/28/nhs_direct_email_data/

[70] J. Thomas, T. Maszczyk, N. Sinha, T. Kluge and J. Dauwels, "Deep learning-based classification for brain-computer interfaces," *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Banff, AB, 2017, pp. 234-239. doi: 10.1109/SMC.2017.8122608

[71] J. Thorpe, P. C. van Oorschot, and A. Somayaji. 2005. Passthoughts: authenticating with our minds. In Proceedings of the 2005 workshop on New security paradigms (NSPW '05). ACM, New York, NY, USA, pp. 45-56. DOI=http://dx.doi.org/10.1145/1146269.1146282

[72] United States, Census Bureau. (2016, April 15). *FFF: Older Americans Month: May 2016*. Retrieved February 13, 2018, from https://www.census.gov/newsroom/facts-for-features/2016/cb16-ff08.html

[73] Van Der Ploeg. (2003). Biometrics and the body as information: Normative issues of the socio-technical coding of the body. In D. Lyon (Ed.), *Surveillance as Social Sorting: Privacy, risk, and digital discrimination*(pp. 57-73). London: Routledge.

[74] Visa Inc.. (n.d.). Consumers preferred biometric authentication methods for payments in the future in Europe as of 2016. In *Statista - The Statistics Portal*. Retrieved March 16, 2018, from https://www-statista-com.libproxy.lib.unc.edu/statistics/728141/biometric-payments-consumers-method-preference-europe/.

[75] Wang, H. A. Abbass and J. Hu, "Continuous authentication using EEG and face images for trusted autonomous systems," 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, 2016, pp. 368-375. doi: 10.1109/PST.2016.7906958

[76] What is the function of the various brainwaves? (1997, December 22). *Scientific American*. Retrieved October 12, 2017, from https://www.scientificamerican.com/article/what-is-the-function-of-t-1997-12-22/

[77] R. J. Williams and D. Zipser, "A learning algorithm for continually running fully recurrent neural networks," *Neural computation*, vol. 1, no. 2, pp. 270–280, 1989.

[78] S. William, and L. Brown (2015). User Authentication. In *Computer Security: Principles and Practice*(3rd ed., pp. 72-110). New Jersey: Pearson Education.

[79] YouGov. (n.d.). How many of your accounts use the same password for online logins?. In *Statista - The Statistics Portal*. Retrieved March 16, 2018, from https://www-statista-com.libproxy.lib.unc.edu/statistics/763091/us-use-of-same-online-passwords/.

[80] J. Yuan, C. -H. Hsieh, and C. -C Chang. (2010). National technology foresight research: A literature review from 1984 to 2005. International Journal of Foresight and Innovation Policy, 6(1), pp. 5–35.