2019 IEEE International Conference on Big Data (Big Data)

An Authentication System using Neurological Responses to Music

Joseph M Cauthen
Department of Computer Science
California State Polytechnic
University, Pomona
Pomona, CA
jmcauthen@cpp.edu

Tejas Gandre
Department of Computer Science
California State Polytechnic
University, Pomona
Pomona, CA
tgandre@cpp.edu

Marco A. Mercado Espinoza
Department of Computer Science
California State Polytechnic
University, Pomona
Pomona, CA
mam@cpp.edu

Meetkumar J Patel
Department of Computer Science
California State Polytechnic
University, Pomona
Pomona, CA
mjpatel@cpp.edu

Mohammad I Husain
Department of Computer Science
California State Polytechnic
University, Pomona
Pomona, CA
mihusain@cpp.edu

***Abstract*—As attacks against password-based authentication increase, the need for robust biometrics becomes apparent. Currently, two of the most popular biometric authentication systems are fingerprint and facial recognition. However, both of these biometrics become unusable once compromised. Also, an attacker might coerce the user to force authentication. Therefore, we propose an authentication mechanism that depends on the participant's neurological responses to chosen pieces of music measured using electroencephalographic (EEG) signals. The current study proposes an authentication system that uses neurological responses to music for classification. Participants listened to individually selected music and music selected by other participants during an EEG reading. The change in the Alpha and Beta band frequencies across seven electrodes served as the input to a user specific K-Nearest Neighbors (KNN). The classifier attempts to determine if we can identify a user based on their EEG response to music. Our pilot data collection and analysis has shown promise of this authentication system with an accuracy rate between 76.4%-92.3%.**

***Index Terms*—authentication, electroencephalography, music, machine learning, classification**

I. Introduction

The amount of login information a user must remember increases as more services rely on passwords, security questions, and pin numbers. As a result, users might choose to use the same login credentials for multiple services. This poses a risk to the user. A single security breach might result in multiple compromises. In 2018, a data breach at Facebook compromised over 50 million user records [1]. In 2017, Yahoo disclosed that a massive data breach exposed over 3 billion user names and passwords [2]. This problem has created new markets for services that assist users in remembering login information such as dependency management systems. New forms of authentication should seek to minimize the expectations of the user.

This work was supported in part by NSF grants CNS-1758017 and DGE-1504526, approved by CPP IRB 19-200.

A. Biometric Authentication & Coercion

Biometric authentication systems offer security without requiring the user to memorize login information. A biometric authentication system relies on the biological characteristics of an individual to verify their identity. Examples of biometrics include fingerprint analysis, facial recognition, and retina scanning.

The strength of biometric authentication comes from the uniqueness of certain biological characteristics. The complexity of forging biological information reduces the chance of biological authentication systems becoming an attack vector. This makes biometric authentication ideal for protecting data that requires high levels of security such as financial, health care, and defense related information.

However, a central problem with current biometric authentication is that once it is compromised, there's no way to update it and it becomes unusable as these are constant biological features of a human being. Also, most biometric authentication will allow an authorized user to access a system regardless of the conditions surrounding why they want to access it. A coercive attack involves the threat of physical harm or force against an authorized user in an attempt to compel that user to access a system on behalf of an attacker [3]. Stress detection might provide an authentication system with the information necessary to prevent this attack.

Various studies have used EEG to detect stress in participants. For example, in [4], researchers built a classifier to detect stress induced by listening to various genres of music. In [5], researchers presented work that correlated changes in frequency bands to stressful tasks. Therefore, in this study we

978-1-7281-0858-2/19/$31.00 ©2019 IEEE

use the EEG responses to the user's chosen pieces of music as an authenticator that can be updated as well as thwart coercion by eliciting signs of stress in the EEG signal.

B. Machine Learning & Authentication

A robust authentication system must prioritize certain attributes. These systems should seek to minimize the number of users falsely accepted in to a system. A system that lets in an unauthorized user poses more risk than one that rejects an authorized user. At the same time the system must maintain high enough accuracy for authorized users to conduct work or use a service without multiple login attempts. The limited availability of training data could pose issues for complex classification algorithms. For these reasons, the current study evaluates the efficacy of the KNN algorithm for music-based EEG authentication.

The KNN algorithm shows promise in classifying certain sets of EEG data. This algorithm classifies new data points based on proximity to existing data points with known classes. This algorithm requires smaller amounts of training data and training time than more complex models such as neural networks.

Existing research supports the efficacy of this model in EEG classification tasks. In [6], researchers were able to classify emotions using a KNN algorithm and 14 sensor headset with a 92.7% accuracy. These findings suggest that this algorithm has the potential to achieve high accuracy in EEG classification tasks, even with a low number of sensors.

In research conducted at the Massachusetts Institute of Technology, seizure classification was performed with patient-specific support vector machines (SVM) with a 96% detection rate. The patient-specific model yielded lower false positives and quicker detection times than a multi-patient algorithm [7]. This work suggests that a user specific-models in EEG data analysis will likely yield higher authentication accuracy rates than a more general classifier.

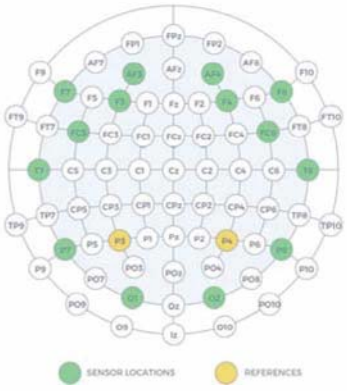

Fig. 1. Emotiv EPOC+ sensor placement diagram. [8]

II. Procedure

A. Data Collection

EEG readings were collected from five participants, four male and one female with a Generation 2, 16 sensor, 128 Hz Emotiv EPOC+ headset as shown in Fig 1. This headset arranges sensors to conform to the 10-20 EEG placement standard. The headset connected through an Emotiv wifi dongle included with the device. The team used the Emotiv Pro software suite to monitor and record readings.

Each participant had four trials. Each trial consisted of five readings, four of which were negative samples and one positive sample. Each reading consisted of 40 seconds of silence and 40 seconds with music without lyrics playing through earphones. This produced 20 readings, 4 in which participant listened to their chosen music and 16 in which they listened to the music of other participants. Thus, in total, we collected 100 readings since the sample size of participants is five.

Participants were asked to follow certain guidelines during the readings. Each reading was conducted while the participant sat in a chair facing away from the researcher. No other people were allowed in the room while the reading was in progress. The participant was instructed to sit with both feet on the floor and arms resting on their thighs. Participants were asked to keep their eyes closed while readings were taken to reduce oculomotor artifacts. The researcher began recording when the EEG amplitudes visibly reduced and stabilized.

$$X_{change} = |X_{music} - X_{silent}| \tag{1}$$

B. Preprocessing

The EEG data was converted from a time series into a time frequency series for analysis using a Morlet transform. The team accomplished this with the MNE Python3 library, version 0.14.0 [9]. Each sensor reading produced an Alpha band and a Beta band series. The Alpha band was defined as frequencies between 8 hertz and 13 hertz and the Beta band between 13 hertz and 30 hertz.

The response to the music was defined as the absolute change in the average frequency between the two readings according to Eq. (1). To limit variation and model complexity, batches of 100 samples were averaged together according to Eq. (2). This process resulted in 28 dimensional feature vectors, two dimensions for each sensor.

$$\hat{X}_i = \frac{1}{100} \sum_{k=1}^{100} X_{(100*i+k)} \tag{2}$$

C. Classification

KNN models were constructed for each participant with the Scikit-learn python3 module, version 0.21.3 [10]. Each model accepted seven dimensional feature vector input. These dimensions comprised the average Alpha band readings from the F4, F7, and F8 sensors, as well as the average Beta band readings from the AF3, AF4, FC5, and F4 sensors. 21 dimensions were excluded based on the contact quality reported by the Emotiv Pro software during readings and the size of the response calculated across all participants.

Feature vectors were constructed by calculating the difference between baseline (silent) reading and response (musical) readings across all sensors using Eq. (1). Feature vectors were

labeled as 1 if the participant listened to their chosen music. This set made up the authorized users samples and represented an authorized user attempting to access a system. The set of vectors derived from readings in which the participant listened to music belonging to other participants were labeled as 0. These vectors made up the attacker samples because they simulated someone other than the authorized user attempting to access a system.

Classification was performed by building a unique KNN model for each user. The authorized user training set consisted of 80% of the total authorized user samples while 20% was used for testing. An equivalent amount of attacker samples were randomly selected from the larger attacker set.

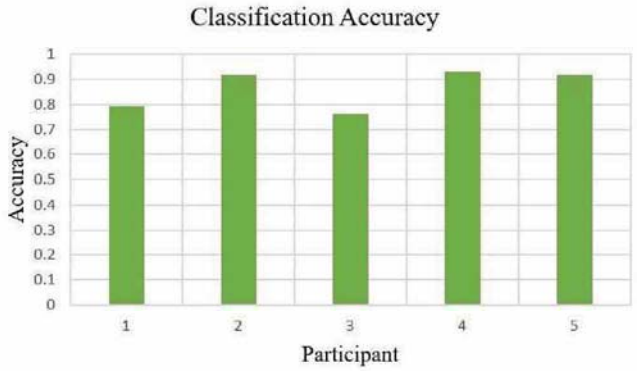

Fig. 2. Identification accuracy of different users based on their EEG responses to music.

III. Results

The five KNN models produced five accuracies, one for each participant. These accuracies ranged from 76.3% to 92.3% with an average of 86.4%. Figure 2 shows the individual results.

Data was visualized using Uniform Manifold Approximation and Projection for Dimension Reduction (UMAP). This algorithm reduces from N dimensional feature vectors to three dimensions while attempting to preserve and represent the most valuable information from the excluded dimensions [11]. In our case, we reduced from seven dimensional feature vectors to three dimensions. Fig. 3 illustrates the UMAP visualization for the highest accuracy model of the participant produced via the method described.

IV. Conclusion

The results obtained here support the hypothesis that authentication systems using the EEG responses to music could be promising. Traditional authentication systems could incorporate the method described in this study as a second factor for systems requiring a high level of security such a military applications or banks.

The accuracies obtained with the KNN classifiers need validation through more robust research design and larger sample sizes. In addition, the model selected here may not represent the most optimal model for this task. Other EEG classification studies have produced high accuracies with models based on the Support Vector Machine (SVM).

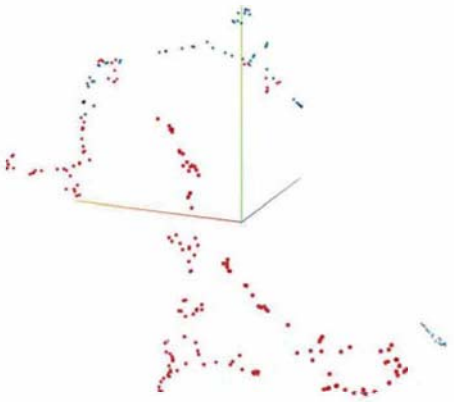

Fig. 3. Uniform Manifold Approximation and Projection for Dimension Reduction (UMAP) applied on a participant's Key EEG (Blue) and Attackers EEG (Red). The two sets exist in distinct locations on the graph with visible separation.

Future research will seek to answer many of the questions that these results raise. Larger sample sizes will test whether this concept generalizes to the population. Blind research designs will minimize the potential of researcher bias and extra environmental precautions will reduce audible and electromagnetic noise. Finally, researchers will test this concept with additional classification algorithms such as SVM.

References

[1] M. Isaac and S. Frenkel. "Facebook Security Breach Exposes Accounts of 50 Million Users". [Online]. Available: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html. [Accessed: 18- Nov- 2019].

[2] R. McMillan, R. Knutson. "Yahoo Triples Estimate of Breached Accounts to 3 Billion" [Online]. Available: https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804. [Accessed: 18- Nov- 2019].

[3] M. Wolotsky, M. Husain and E. Chloe, "Chill-Pass: Using Neuro-Physiological Responses to Chill Music to Defeat Coercion Attacks," 2014.

[4] A. Asif, M. Majid, and S. M. Anwar, "Human stress classification using eeg signals in response to music tracks," *Computers in biology and medicine*, vol. 107, pp. 182–196, 2019.

[5] M. A. Hafeez, S. Shakil, S. Jangsher, "Stress effects on Exam Performance using EEG", 14th IEEE International Conference on Emerging Technologies, pp. 1-4, 2018.

[6] M. Li, H. Xu, X. Liu and S. Lu "Emotion recognition from multichannel EEG signals using K-Nearest Neighbor classification," in Technology and Health Care, vol 26., pp. S509 - S519, 2018.

[7] S. A. Hossam, "Application of machine learning to epileptic seizure onset detection and treatment," Sep 2009.

[8] "EMOTIV EPOC+ 14 Channel Mobile EEG," EMOTIV. [Online]. Available: https://www.emotiv.com/product/emotiv-epoc-14-channel-mobile-eeg/. [Accessed: 18-Nov-2019].

[9] A. Gramfort, M. Luessi, E. Larson, D. Engemann, D. Strohmeier, C. Brodbeck, R. Goj, M. Jas, T. Brooks, L. Parkkonen, M. Hämäläinen, MEG and EEG data analysis with MNE-Python, Frontiers in Neuroscience, Volume 7, 2013, ISSN 1662-453X, [DOI]

[10] Pedregosa F, Varoquaux, Gael, Gramfort A, Michel V, Thirion B, Grisel O, et al. Scikit-learn: Machine learning in Python. Journal of machine learning research. 2011;12(Oct):2825–30.

[11] L. McInnes, J. Healy and J. Melville, "UMAP: Uniform Manifold Approximation Projection for Dimension Reduction," Dec 2018.