# IoT Two Factor Neurometric Authentication System using Wearable EEG

Angel Rodriguez Sara Rampazzi Kevin Fu
*University of Michigan - Ann Arbor*
Ann Arbor, Michigan, United States of America
{angelrod, srampazz, kevinfu}@umich.edu

***Abstract*—The IoT authentication space suffers from various user-sided drawbacks, such as poor password choice, the accidental publication of biometric data, and the practice of disabling authentication completely. This is commonly attributed to the *Security vs Usability* problem - generally, the stronger the authentication, the more inconvenient it is to perform and maintain for the user. Neurometric authentication offers a compelling resistance eavesdropping and replay attacks, and the ability for a user to simply *think to unlock*. Furthermore, the recent increase in popularity of consumer EEG devices, as well as new research demonstrating its accuracy, have made EEG-based neurometric authentication much more viable. Using a Support Vector Machine and one-time tokens, we present a secure two-factor authentication method, that allows users to authenticate multiple IoT devices. We perform preliminary trials on the Psyionet BCI dataset and demonstrate a qualitative comparison of extracted EEG feature sets.**

***Index Terms*—Security, EEG, IoT Authentication, Machine Learning, Brain Computer Interface, Wearables**

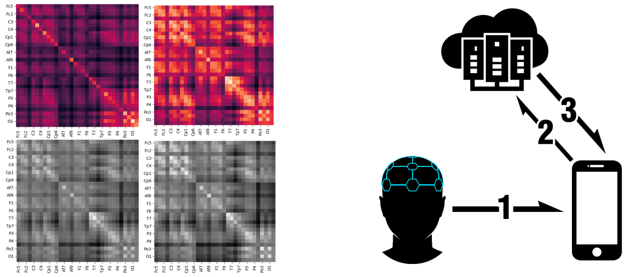
## I. Introduction and Background

In general, vulnerabilities in biometric authentication systems rely on the attacker having some knowledge of the victim's authentication data, such as eavesdropping attacks, or using data Morphing techniques [1]. Consequently, neurometric authentication can provide a resistance to these exploits due to it's need for prolonged physical contact. Using a Riemannian Geometry based feature extraction algorithm [2], and a Support Vector Machine, we present a secure two factor authentication, that allows users to authenticate multiple IoT devices with the same platform. By utilizing one-time tokens, our method does not need to transmit the users biometric data, while adding a second layer of authentication. One of our preliminary findings (Figure 1(a)) demonstrates distinguishable differences between the extracted features of two different users performing the same mental task, and one user thinking performing two separate mental tasks.

## II. Two Factor Authentication Process

In the preliminary phase, the EEG system is trained to verify the user identity and associate the users different thoughts to different IoT devices. As shown in Figure 1(b), the user control flow is delineated in the following steps:

1) After internal user-though authentication, the device securely sends a one-time token to the IoT device (using Bluetooth, NFC, etc.).
2) The IoT device securely communicates with a server to verify the token, which contains a copy of the seed generated after the training phase.
3) If the token is verified, the server sends a secure confirmation reply to the IoT device, authenticating the user.



(a) (b)

Fig. 1. In figure (a), the top row shows the averaged covariance matrices of the extracted features for two different users thinking about the same mental task (imagining closing their hands). The bottom row shows the averaged covariance for one user thinking of two different tasks (imagine closing both fists vs both feet). Figure (b) shows the EEG two factor authentication phases.

## III. Discussion and Future Work

We outline an EEG-based two factor authentication system. Our methodology benefits from the ability to be implemented without significant computational overhead, making it applicable to the majority of the IoT devices. Recent works demonstrate the high accuracy of live EEG authentication [3], and a compelling in-ear EEG system [4]. Future work includes implementing this methodology using an in-ear EEG and evaluating its accuracy and usability.

## References

[1] M. Gomez-Barrero, C. Rathgeb, U. Scherhag, and C. Busch, "Predicting the vulnerability of biometric systems to attacks based on morphed biometric information," *IET Biometrics*, 2018.

[2] M. Congedo, A. Barachant, and R. Bhatia, "Riemannian geometry for eeg-based brain-computer interfaces; a primer and a review," *Brain-Computer Interfaces*, vol. 4, no. 3, pp. 155–174, 2017.

[3] I. Jayarathne, M. Cohen, and S. Amarakeerthi, "Survey of eeg-based biometric authentication," in *Awareness Science and Technology (iCAST), 2017 IEEE 8th International Conference on*. IEEE, 2017, pp. 324–329.

[4] M. T. Curran, N. Merrill, J. Chuang, and S. Gandhi, "One-step, three-factor authentication in a single earpiece," in *Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers*. ACM, 2017, pp. 21–24.