Brainer - User authentication using brain waves

Akshay Muraleedharan Nair Santhy
akshayms@asu.edu
1212981859

Bharath Gunari
bgunari@asu.edu
1213217679

Sameer Kulkarni
sdkulka4@asu.edu
1213232109

Mugdha Kolhe
mkolhe@asu.edu
1213204731

Abstract- This application enables user to login into an android application by just being himself instead of remembering passwords. In this application, we enable user authentication using the user's brain waves. We have collected sample subject data from www.physionet.org. We have then applied machine learning techniques such as KNN, SVM, Decision Tree, Logistic Regression, Naïve Bayes classifier from scikit-learn library to authenticate the user.

I. INTRODUCTION

Brain sensing and associated cognitive applications are fast becoming pervasive in nature due to the advent of wireless low cost easy-to-wear brain sensors such as Neurosky sensor that connect to mobile phones. This enables seamless access to a person's brain waves which contains information that is unique to a person, nearly impossible to impersonate without invading personal space, and chaotic over time. In recent times, we have seen new biometric authentication systems like TouchID, FaceID and Iris scanner.

Bank transactions are based on these new authentication systems. Hence we are experimenting on a new type of biometric authentication system based on EEG signals.

II. AUTHOR KEYWORDS

Authentication, Machine learning, Biometric authentication, EEG, Brain Signals, Fog, Cloud.

III. PROJECT REQUIREMENTS

1. Cloud server must have python3, with pandas, scipy, numpy and sklearn libraries installed.
2. Cloud server must have nodejs and nodejs-express installed.

IV. ARCHITECTURE

In order to set up the web server on both the back-ends (Fog and Cloud), we have used nodejs server. A node js instance is running on both fog and cloud servers. Fog server is set up on Ubuntu 16.04 LTS on laptop and cloud server is set on Ubuntu on Amazon Web Services (AWS).

The android application sends the algorithm name and user data to the servers. The mobile app can also calculate the computation and communication latency and suggest the user which the server to choose for authentication. The file connapp.js will be listening in the server at port 3000 all the time during testing. The server runs the appropriate algorithm on the server and returns the results to the android application.

According to the user's choice, the phone sends the data to Fog or the Cloud server. The server tests the data, and identifies the user and then, the android application will unlock.

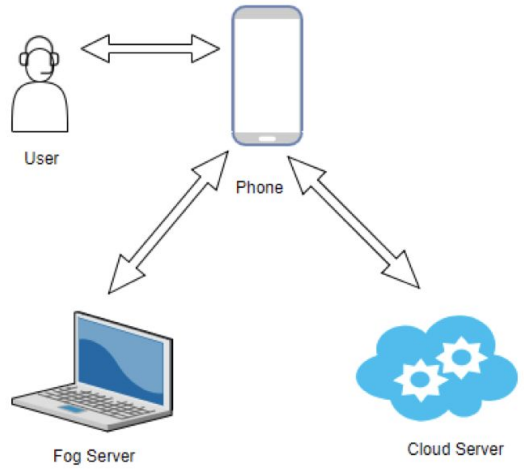

Fig. 1: Architecture

V. DATA COLLECTION

We have collected online sample subject data from www.physionet.org. A total of 64 data samples of four subjects with opened eyes and closed eyes each was used. The dimension of the training data was 512*9760, since there were (64*4=512) samples and 9760 features. A total of five random samples are considered for test data. Therefore, dimension of test data is 5*9760. Test data and training data have no overlapping data entries. The fifth user's data (Unknown_Subject) is not used in training, hence, the authorization will fail for that user as demonstrated in Fig. 5.

Since we were testing on the same sample data we are getting very good accuracy rates.

VI. IMPLEMENTATION

Firstly, the user's brain wave signals are taken and authenticated in real time using 5 different machine learning algorithms, namely, KNN, SVM, Decision Tree, Logistic Regression, Naïve Bayes classifier from scikit-learn library. Since no working sensor were available, sample data of 4 subjects are used and added in a drop down list. For each user name selected, the respective persons EEG data which be chosen. The user can then choose the algorithm and processing environments (mobile, fog, cloud or automatic) for authentication. The mobile will look at the latency rate of both and decides which one to use in order to authenticate. We recommend using the automatic option as it will choose the environment with lowest computation and communication latency (pending). Once authenticated successfully, user will get a success message else a failure message.

A. User Interface Options

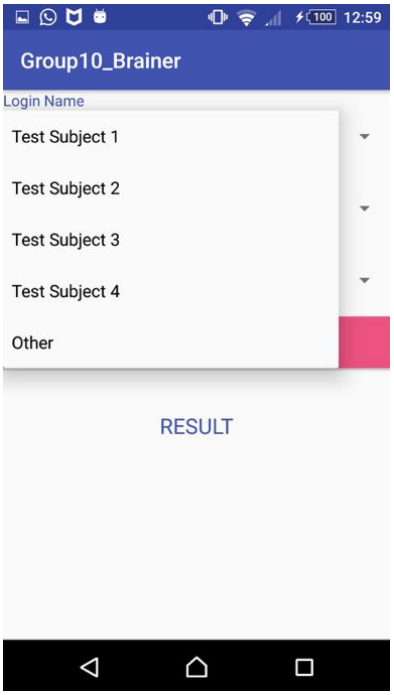

Fig. 2: User options for selecting user for authentication process

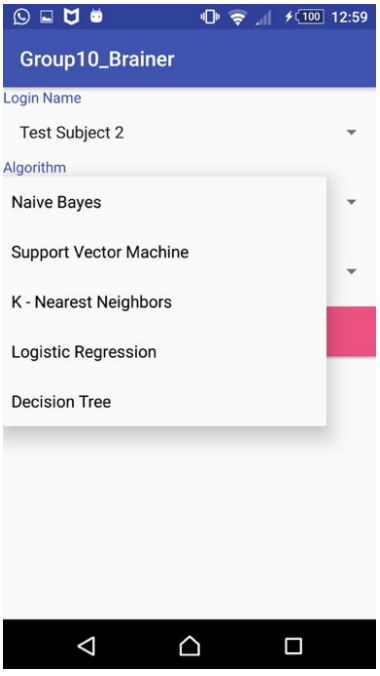

Fig. 3: User options for selecting algorithms for authentication process

B. User Authentication

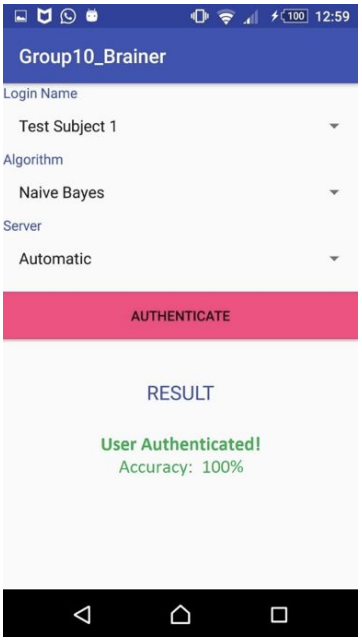

Fig. 4: Successful authentication

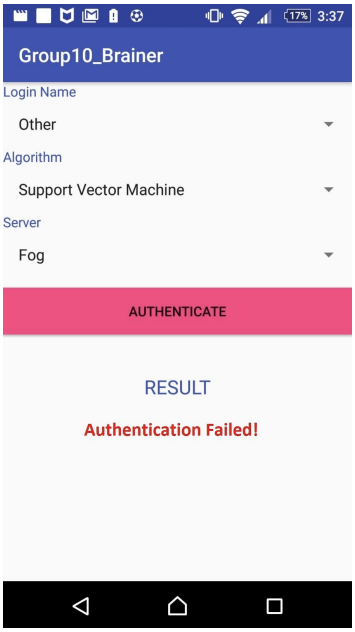

Fig. 5: Unsuccessful authentication in case of a user who is not a contributor to the training data.

C. FOG AND CLOUD AUTHENTICATION

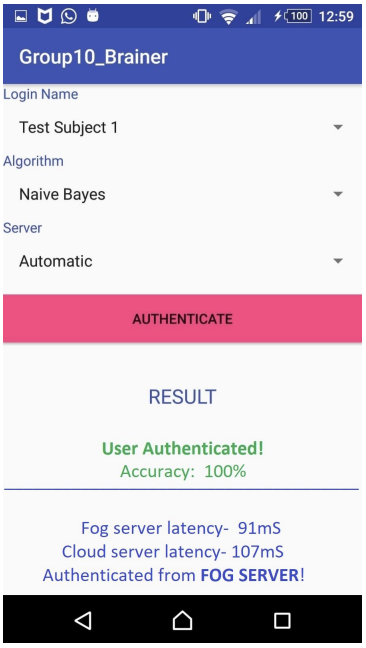

Fig. 6: Automatic server selection

VII. LIMITATIONS

We have trained the algorithm with data collected from the users and used that knowledge to authenticate the users. Hence, we were able to achieve excellent accuracy. We could not test the application with real time data since the sensors had some issues. We probably would have achieved less accuracy with real time data just as with the case of touch ID and faceID. But this way of authenticating is hassle free and quicker when compared to traditional way of unlocking using passcode.

VIII. CONCLUSION

In this project we have used EEG signals to authenticate the user. The process involves getting the brain signals from the users and authenticate them. This is a time consuming process. Hence we have designed the algorithm which decide s whether the system should use fog server or a cloud server to authenticate. This is a valuable addition to already existing authentication methods using biometrics and can be used in financial institutions, phones etc in the future.

IX. ACKNOWLEDGEMENT

We would like to thank Dr. Ayan Banerjee for guiding us throughout this project. We also would like to thank the TA Koosha Sadeghi for providing us with the test data. We have learnt many concepts and technologies while developing this application.

X. REFERENCES

- Goldberger AL, Amaral LAN, Glass L, Hausdorff JM, Ivanov PCh, Mark RG, Mietus JE, Moody GB, Peng C-K, Stanley HE. PhysioBank, PhysioToolkit, and PhysioNet: Components of a New Research Resource for Complex Physiologic Signals. Circulation 101(23):e215-e220 [Circulation Electronic Pages; http://circ.ahajournals.org/cgi/content/full/101/23/e215]; 2000 (June 13).
- Javad Sohankar, Koosha Sadeghi, Ayan Banerjee, and Sandeep K.S. Gupta. 2015. E-BIAS: A Pervasive EEG-Based Identification and Authentication System. In Proceedings of the 11th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet '15). ACM, New York, NY, USA, 165-172. DOI= http://dx.doi.org/10.1145/2815317.2815341
- EEG Recording and Online Signal Processing: https://www.hindawi.com/journals/bmri/2017/3072870/
- Real time analysis of EEG signals on Androidapplication: https://ieeexplore.ieee.org/document/7002387/