Leveraging Movement, Posture, and Anthropometric Contexts to Strengthen the Security of Mobile Biometrics

Robert Eslinger, Kiran Balagani, Paolo Gasti, Rosemary Gallagher, Isaac Kurtzer
New York Institute of Technology
reslinge@nyit.edu, kbalagan@nyit.edu, pgasti@nyit.edu, rgalla01@nyit.edu, ikurtzer@nyit.edu

Abstract

Behavioral biometrics are characteristics of human behavior (such as how a user swipes on their smartphone) that can be used to authenticate individuals in smartphone security applications. Behavioral biometrics have many advantages compared to physical biometrics, primarily because they can be captured transparently, i.e., without interrupting the user activity. However, because of the noisy nature of these signals, behavioral biometric authentication systems tend require 20-60 second to achieve good performance. During this time window the adversary can, for instance, gain access to a substantial amount of information.

In this work we investigate the limits of authentication performance using signals from the user's posture during smartphone usage. Specifically, we use 3D motion capture to determine whether posture signals have the ability to reliably authenticate users within time windows as short as 5 seconds. Our work leverages expertise in behavioral authentication, neurosciences, and physical therapy to provide a scientifically-grounded view on the temporal performance of posture signals.

Background

Authentication:
In a security context, *authentication* is the process of verifying that a user is who they say they are. One common form of smartphone authentication is the passcode. The issue with security measures like passcodes is that anyone with the information can access the system; there is no check that it is actually the device's owner entering the correct passcode.

Biometric Authentication:
Using biometrics (physiological characteristics such as facial geometry and fingerprints) to verify users. With these systems, it is difficult to replicate an exact physical feature of someone. An example is Apple's Face ID, which scans your face to verify you are the owner.

Behavioral Biometric Authentication:
Using behavioral biometrics to authenticate user identities. The benefit this has is twofold:

1. Authentication is *implicit* – the user does not need to take any inconvenient security steps (like reentering passcode), their identity can be authenticated automatically without their effort.
2. Authentication is *continuous* – the user of the device can be continually verified. This is very relevant to intrusion, as even if an intruder accessed the device through a passcode, the device could still detect that it is an intruder using the phone.

Posture Signals and Authentication Time

The objective of this project is to investigate whether behavioral biometric signals extracted from dynamic posture information can be used to authenticate users within a very short timespan. To this end, we captured full-body 3D motion capture data while users performed common smartphone activities, such as typing text and moving UI elements on the screen via swipes. We hypothesize that posture signals capture quasi-static behavioral characteristics that are unique and stable over time. Our experiments confirm this, and show how even 5 seconds of data can be used to reliably authenticate users. (See Results section.)

This work considers posture features as standalone features *and* to augment traditional movement and swipe features (our baseline). In both cases, posture features performed well in short time window, and provided limited-to-no improvement when extending the authentication window to up to 60 seconds. This shows that posture signals are stable.

The use of 3D motion capture allowed us to determine the limit of posture signal, i.e., without well-known constraints associated with capturing the same signals using body-worn sensors such as smart watches. In particular, under these conditions our experiments demonstrated that posture signals collected from the center portion of the body lead to significantly lower error rates compared to signal from the upper and lower body. This has implications on the type of sensors that should be used to capture posture data with the purpose of continuous authentication.

Data Collection Apps

These apps were developed to obtain phone usage information from the user during experiments. They both record accelerometer, gyroscope, and face-tracking data, as well as video from the front facing camera. They are native iOS apps, written using the Swift language in Xcode.

Typing App:

In this app, the user is prompted to answer basic questions, of which she must respond with a minimum of ten characters. Once she finishes responding, she hits the 'Next' button, and is brought to a new question. The questions are shuffled in a specific order based off the user's experimental ID, in order to ensure the same question never occurs more than once. This app also records all of the keystrokes entered by the user (characters, spaces, backspaces, etc.).

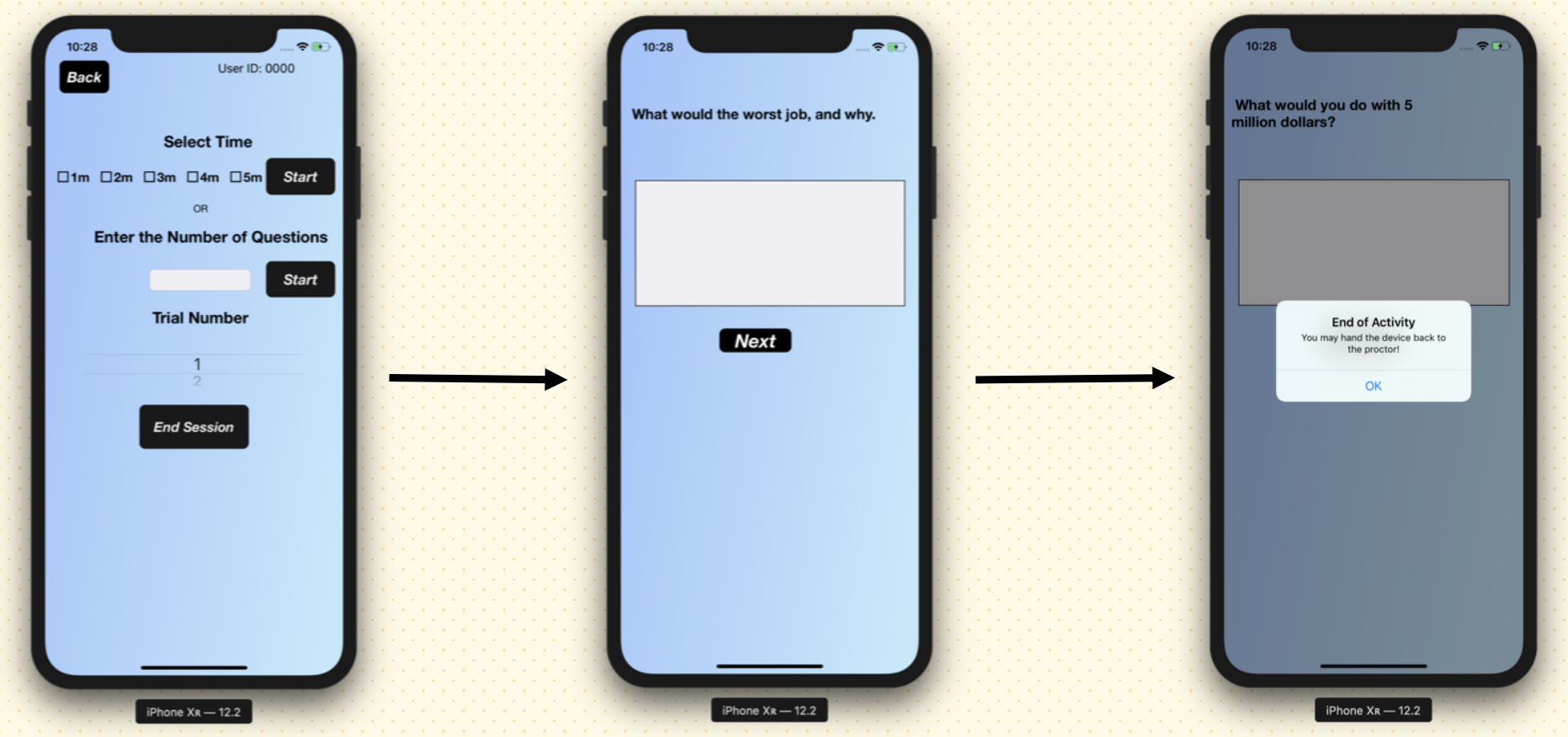

Figure 1. The UI of the typing app. The first screen (left) is only used by the proctor. The participant then hits 'Start', and answers questions until the trial is up, at which time the alert in screen 3 (right) appears.

Swiping App:

In this app, the user is presented with the name of a color (either Blue, Green, Red, or Yellow), whose font is also one of those four colors. Her task is to drag the word to the border corresponding to the color name, not the font color (e.g. if the word 'Blue' popped up in a green font, she would drag that word to the blue border). Once the word touches the correct border, it disappears, and a new word appears. This app also records all of the swipe data of the user, documenting where the user's finger is on the screen, and at what times, during all swipes.

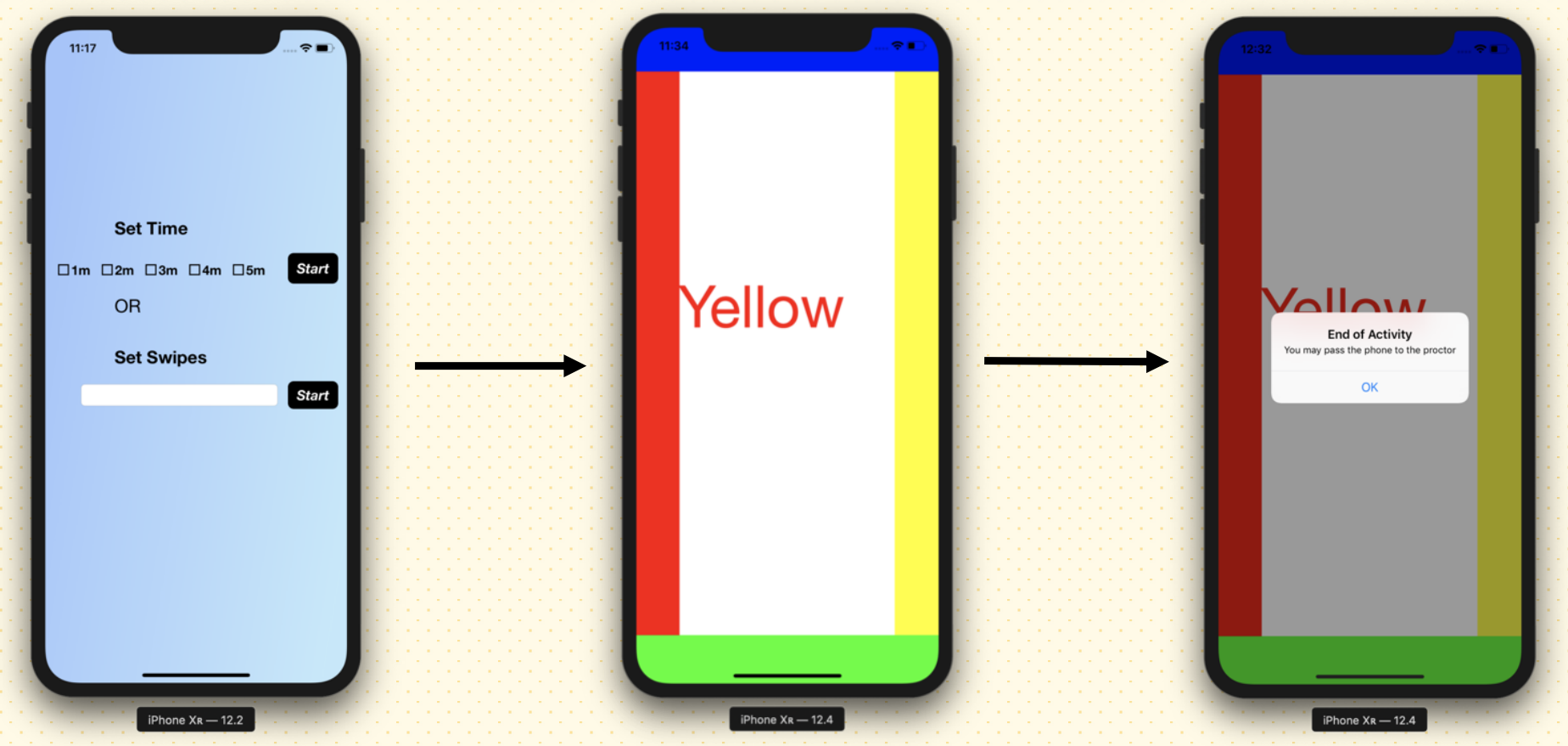

Figure 2. The UI of the swiping app. The first screen (left) is only used by the proctor. The participant then hits the 'Start' button, and drags words trial is up, at which time the alert in screen 3 (right) appears.

Experiment Setup

Figure 3. The Motion Capture Studio, as seen from the ground floor. The bright red lights are the IR illumination LEDs mounted on the Vicon cameras.

Figure 4. User set-up for data collection. The silver spheres taped to the subject are the sensors monitored by the cameras.

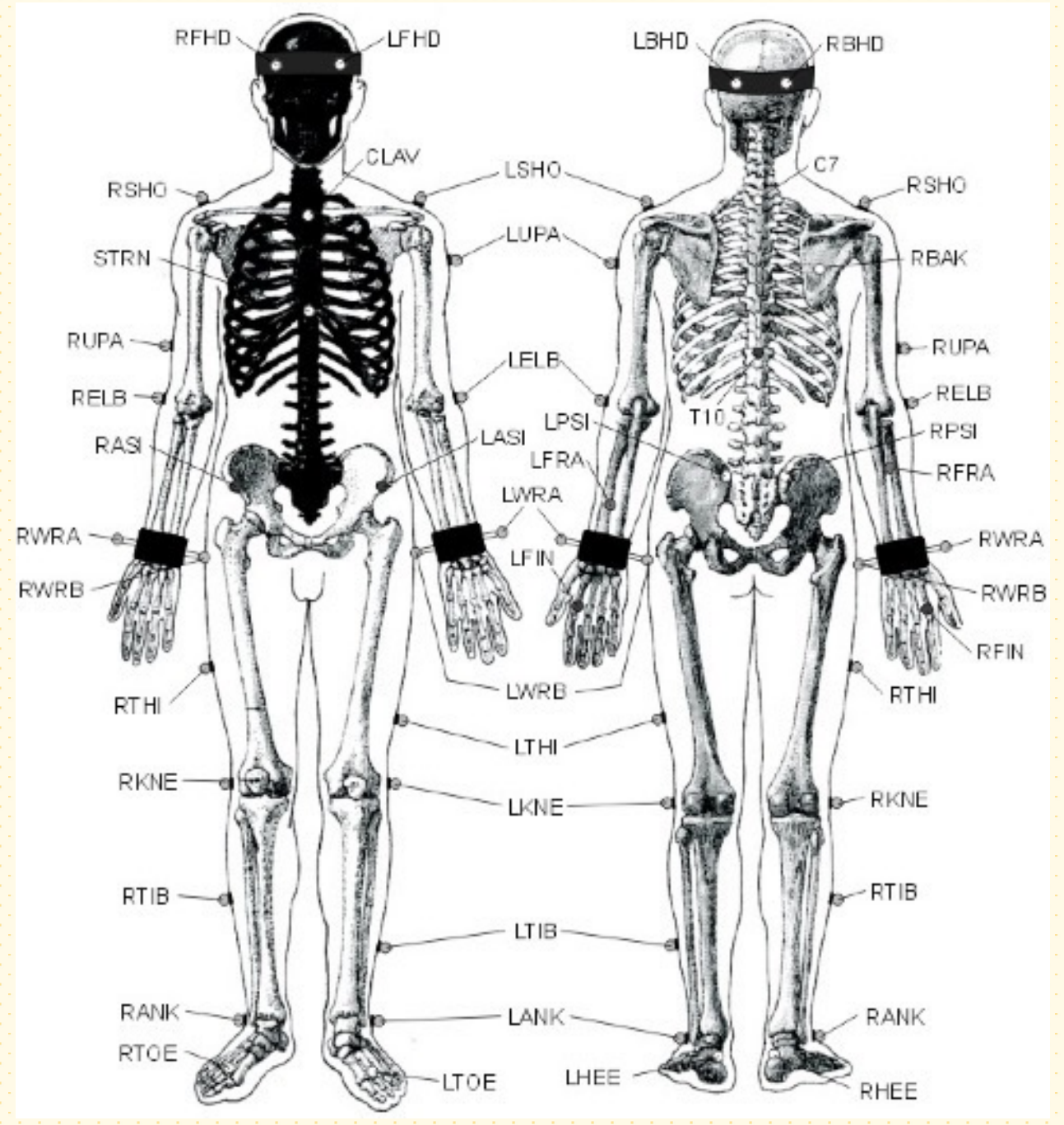

Figure 5. Set of markers used during the experiments

The experimental portion of this research was conducted at the Motion Capture Studio on New York Institute of Technology's campus in Old Westbury, Long Island. The studio is equipped with 36 cameras, which track sensors on the subjects as they move around the studio. This data is then fed to a computer, which produces the real-time video of the subject moving, as seen in Figure 6 (walking) and Figure 7 (sitting). The subjects wore 30+ sensors to be tracked by the motion cameras, as seen in Figure 5, and 3 sensors were placed on the phone as well. The users participated in 2 sessions (one on each of two different days), and during each session completed 12 1-minute trials of each app, 6 trials walking and 6 trials sitting.

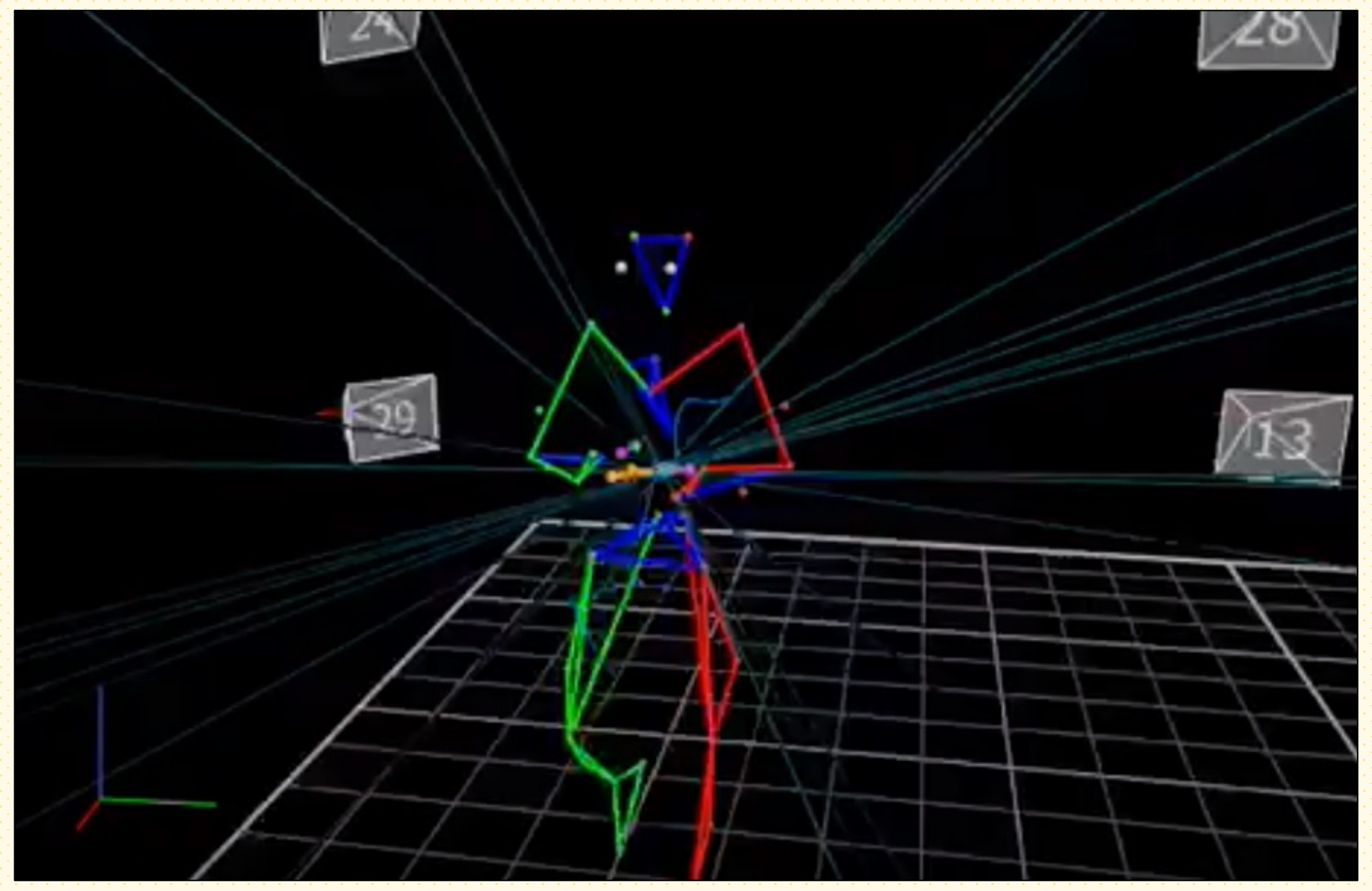

Figure 6. A visualization of the motion capture data during a walking trial. The lines connect 2 sensors on the body, and the numbered, gray squares in the background represent the cameras.

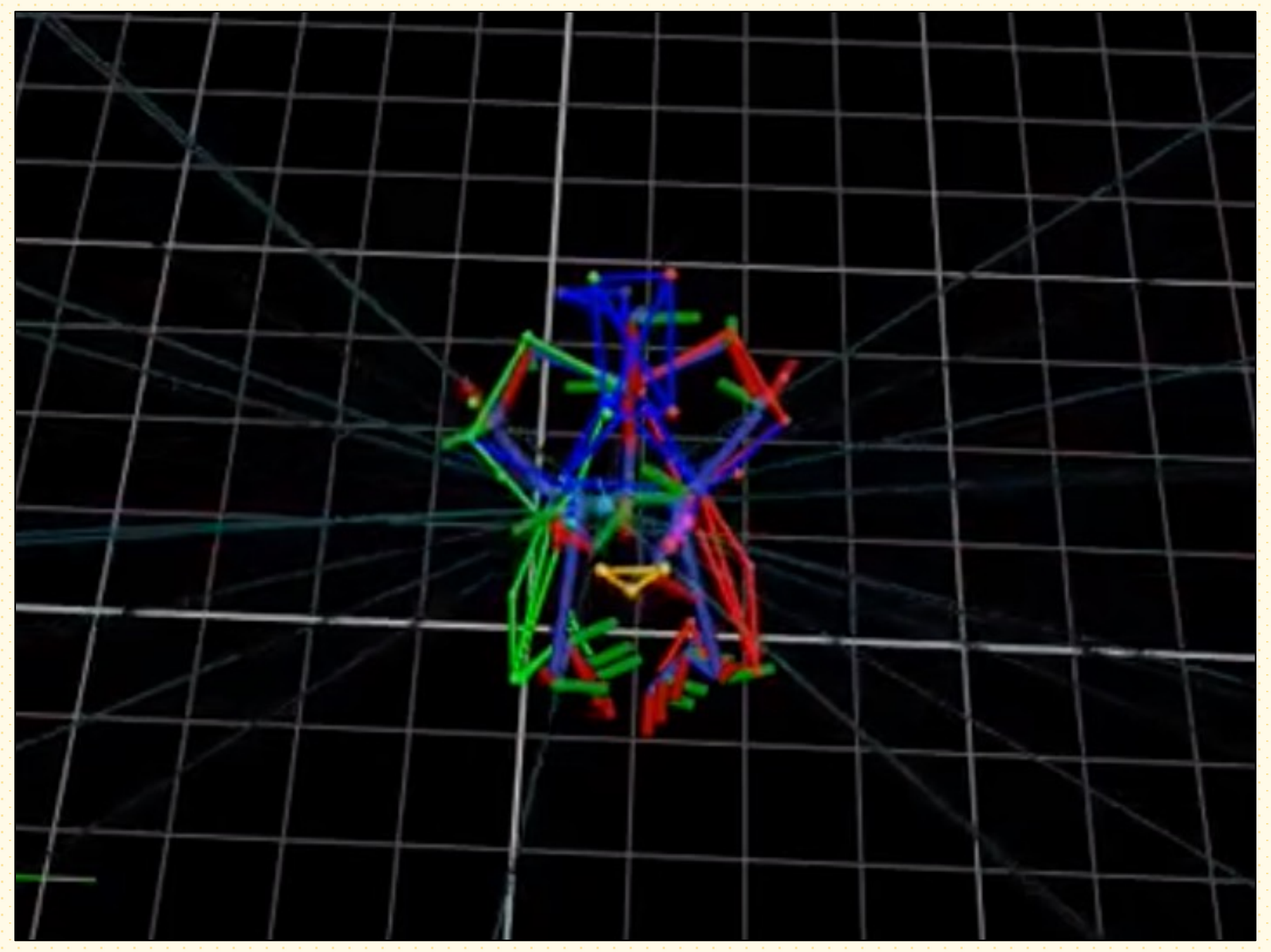

Figure 7. A visualization of the motion capture data during a sitting trial. As in Figure 10, the lines connect 2 sensors on the body.

Results

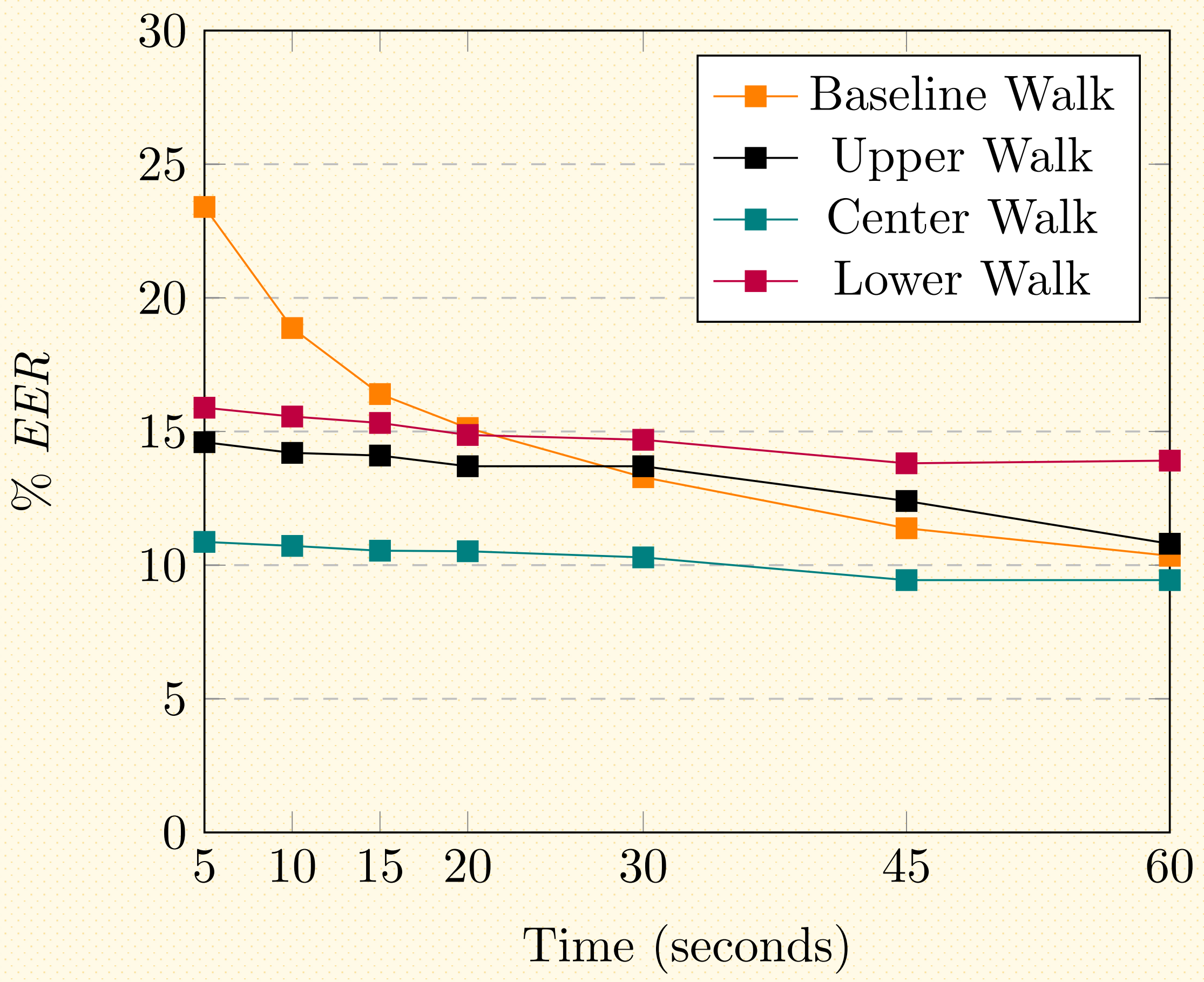

Figure 8. Authentication performance of touchscreen and movement features (Baseline) compared to upper, center, and lower body posture features. During data collection, the user was interacting with the smartphone while walking in the data collection room.

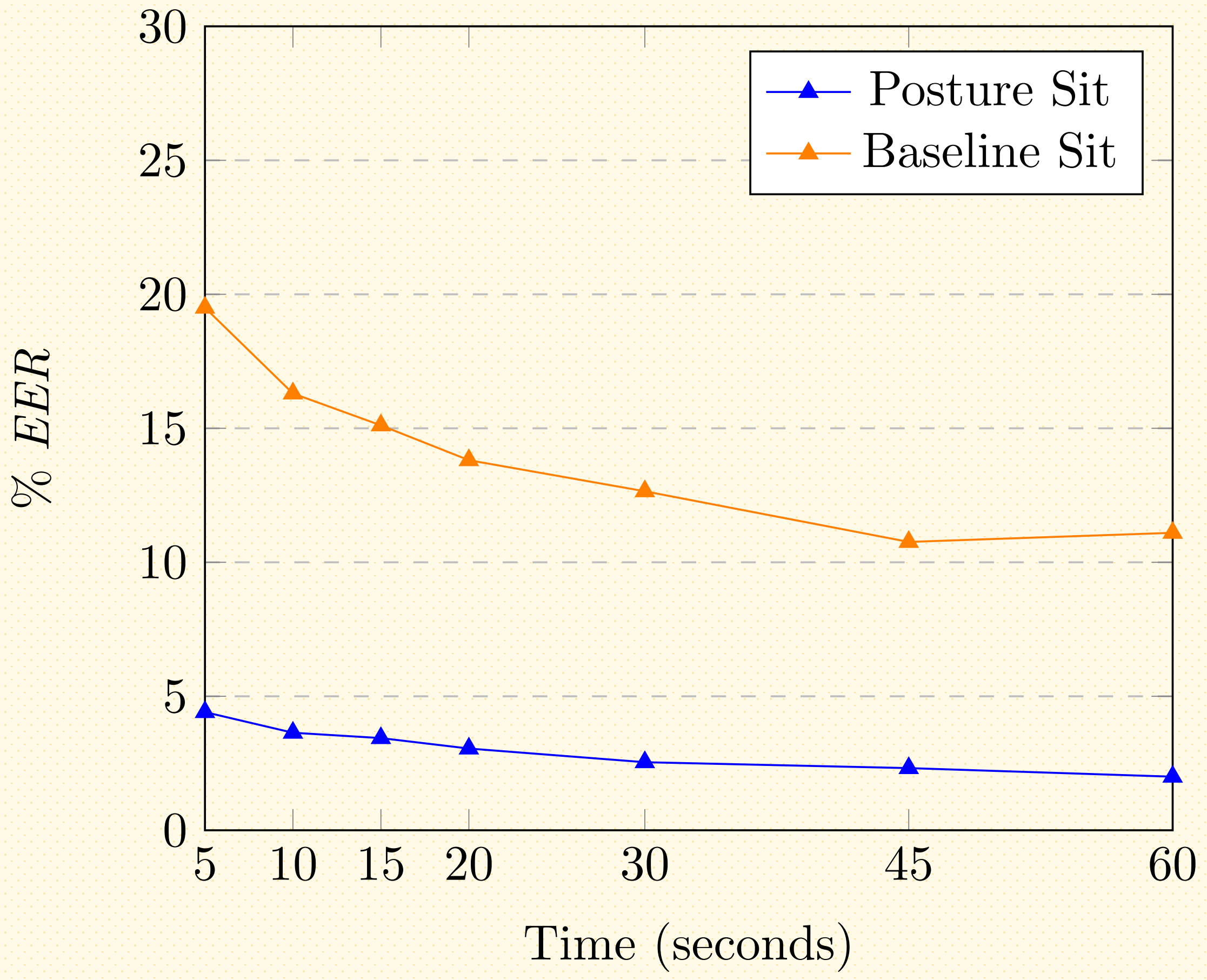

Figure 9. Authentication performance of touchscreen and movement features (Baseline) compared to upper, center, and lower body posture features. During data collection, the user was interacting with the smartphone while sitting.

Acknowledgement

This research was supported by the National Science Foundation (NSF) Research Experiences for Undergraduates (REU) program at the New York Institute of Technology (NYIT) and NSF grant nos. 1852316 and 1619023.

References

[1] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, pages 136 – 148, 2013.
[2] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, Jan. 2015.
[3] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users," IEEE Transactions on Information Forensics and Security, Vol. 11, No. 5, May 2016.