# Thinking Unveiled: An Inference and Correlation Model to Attack EEG Biometrics

DIKSHA SHUKLA, University of Wyoming
PARTHA PRATIM KUNDU, Institute for Infocomm Research
RAVICHANDRA MALAPATI and SUJIT POUDEL, Syracuse University
ZHANPENG JIN, University at Buffalo, SUNY
VIR V. PHOHA, Syracuse University

Very few studies have explored linkages between physiological, such as electroencephalograph (EEG), and behavioral patterns, such as wrist movements. These linkages provide us a unique mechanism to predict one set of patterns from other related patterns. Unlike conventional biometrics, EEG biometrics are hard to spoof using standard presentation attack methods, given the intrinsic liveness resulting from the bounded randomness of EEG signals specific to an individual. In this article, we propose a novel attack on the EEG-based authentication systems by investigating and leveraging the strong correlation between hand movements and brain signals captured through the motion sensors on a smartwatch and the wearable EEG headset, respectively. Based on this technique, we can successfully estimate the user's EEG signals from the stolen hand movement data while the user was typing on the keyboard. Our attack results on the EEG biometric authentication system show an increase in the mean equal error rates of the classifiers by between 180% and 360% based on a dataset of 59 users. In summary, our pilot study calls for a rethinking of EEG-based authentication mechanisms from the perspective of unique vulnerabilities, particularly for multimodal biometric systems involving a variety of wearable or mobile devices.

CCS Concepts: • **Security and privacy** → **Authentication**; **Biometrics**; **Authorization**; *Cryptanalysis and other attacks*;

Additional Key Words and Phrases: Authentication, attack, wearable devices, EEG, security, and motion sensors

**ACM Reference format:**
Diksha Shukla, Partha Pratim Kundu, Ravichandra Malapati, Sujit Poudel, Zhanpeng Jin, and Vir V. Phoha. 2020. Thinking Unveiled: An Inference and Correlation Model to Attack EEG Biometrics. *Digit. Threat.: Res. Pract.* 1, 2, Article 9 (May 2020), 29 pages.
https://doi.org/10.1145/3374137

This work was supported in part by the National Science Foundation (NSF) under grants SaTC-1527795 and CNS-1840790.

Authors' addresses: D. Shukla (corresponding author), Department of Computer Science, University of Wyoming, Laramie, WY 82072; email: dshukla@uwyo.edu; P. P. Kundu, Agency for Science, Technology and Research (A*Star), Institute for Infocomm Research, Singapore; email: partha_pratim_kundu@i2r.a-star.edu.sg; R. Malapati, S. Poudel, and V. V. Phoha, Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY 13210; emails: {rmalapati, spoudel, vvphoha}@syr.edu; Z. Jin, Electrical Engineering and Computer Science, University at Buffalo, SUNY, Buffalo, NY 14260; email: zjin@buffalo.edu.

2576-5337/2020/05-ART9 $15.00
https://doi.org/10.1145/3374137

## 1 INTRODUCTION

Recent research has explored many new physiological and behavioral biometrics for authentication purposes, including the electroencephalograph (EEG) and hand movements, both of which provide viable signals that can be used to verify a user's identity [36, 39, 40, 44, 49, 53]. In particular, EEG-based biometrics have been proven in prior studies to be effective, reliable, and controllable, possessing unique advantages over other conventional biometrics, due to its intrinsic liveness indication and cancelable nature [25, 30, 41]. However, as an emerging biometric approach, the security and vulnerability of EEG biometrics are largely underexplored and incompletely understood. Given the unique generation and characteristics of EEG signals, it has been well acknowledged that it is extremely challenging to impersonate someone to spoof EEG biometric authentication systems using artificially synthesized EEG signals [15, 47].

Toward this aim, we seek to investigate the vulnerability of EEG-based authentication systems and explore alternative ways to break into the authentication protocol using fake EEG templates created through the strong correlation between the activities of networks of neurons within the brain and neuromuscular system [13]. Therefore, the following questions need to be considered: (1) Does the brain affect (measured through EEG) the hand movements (measured through an accelerometer and gyroscope) during typing? and (2) Is there any correlation between the brain activities and the hand movements? The uniqueness of our work stems from providing empirical evidence that this relationship exists and can be captured through readings of wearable devices such as NeuroSky or the Emotiv Epoc+ headset and the smartwatch in a meaningful way, as well as demonstrating that the relationship has enough fidelity to infer one signal from the other. We posit that this work opens up a new class of attacks on biometrics because of the inherent relationships present in different modalities of biometrics and the human brain, which is a source of additional biometrics.

Specifically, we present an attack on EEG-based authentication systems that exploits the correlations between brainwave signals and hand movements. Our attack requires only the hand movement data of the victim and the correlation model established based on a training dataset obtained using a NeuroSky or Emotiv Epoc+ headset for brain waves and a Sony smartwatch for hand movements. Figure 1 shows an example scenario of the experimental setup for the data collection procedure in our laboratory. Brainwave signals and the hands movements were captured for each volunteer participants while they performed a given set of activities. In the first phase of data collection, the participants wore the given smartwatch in the hand of their choice. The hand movements were recorded for all the participants to analyze its correlation with the corresponding brainwave signals. In the second phase of data collection, the participants wore smartwatches in both the hands. The movements of both hands were recorded in the second phase of experiments to analyze and compare the interrelations of brainwave signals with left hand movements and with right hand movements.

Figure 2 shows the process flow of our attack model. An attacker gains access to the publicly available population dataset of hand movements and the corresponding brainwave signals. The attacker establishes the correlation model between the two signals. The attacker also snoops the hand movements of the victim using a snooping technique (e.g., by installing a malicious application on the user's smartwatch or by eavesdropping keyboard acoustic emanations [10, 27, 33, 54]). Once the attacker gets access to the victim's hand movements, she or he generates the corresponding fake EEG signals and then feeds the generated fake signals to the victim's EEG-based authentication system to gain access to the user's device.

We evaluated the performance of the proposed attack scheme and presented the results based on the dataset collected from 59 volunteer participants in two separate sessions: the training session and the testing session. In each session, each participant was assigned two randomly selected videos: the first video from the pool of happy videos and the second from the pool of sad videos. The pool of videos consisted of 40 short, publicly available YouTube videos that we selected based on happy or sad emotional content in the videos (see Appendix A). Participants were asked to first watch the first video for 300 seconds and then type their responses to various

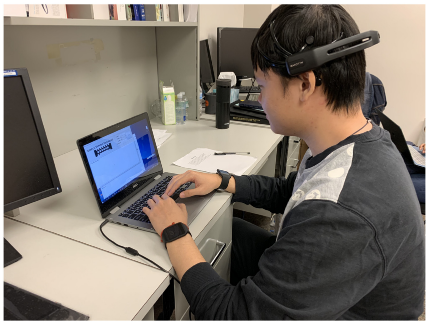


Fig. 1. Experimental setup. A user is typing on his laptop, and the brainwave signals are being captured using a 14-channel Emotiv Epoc+ headset. The hand movements are being captured using Sony smartwatch motion sensors that the user wore on his wrist. Data collection experiments were conducted in two separate phases. Although the figure shows EEG data recording using the Emotiv Epoc+ headset, phase I data collection experiments were conducted using a NeuroSky headset, whereas EEG data in phase II was collected using an Emotiv Epoc+ headset. In addition, hand movements from one hand of the user were recorded in phase I experiments, whereas movements of both hands were captured in phase II experiments.

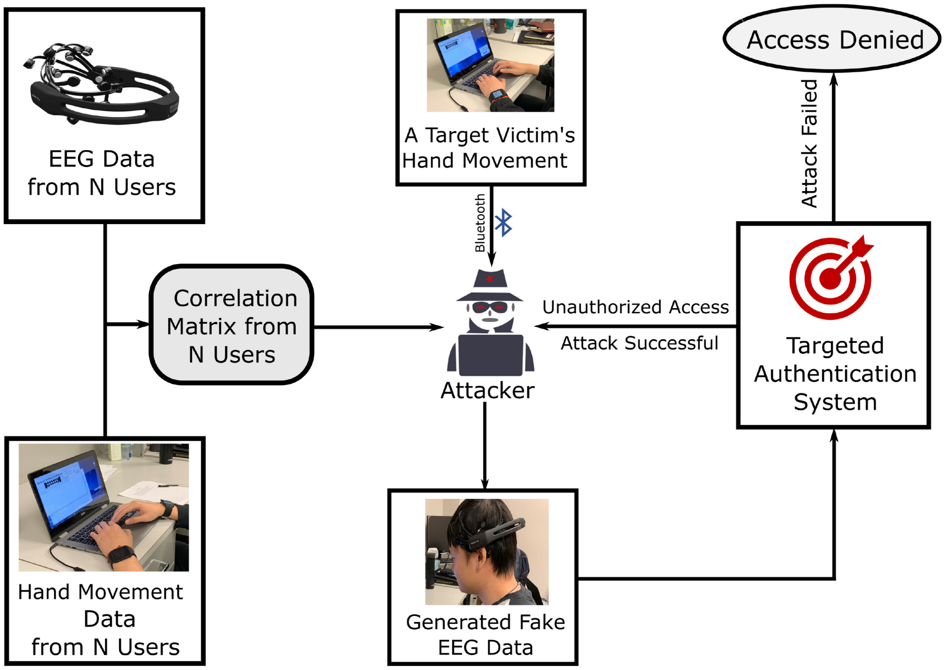


Fig. 2. Attack model. The correlation matrix is computed using the EEG signals and hand typing patterns based on the population data (N users). The attacker snoops the targeted user's hand movements and generates fake EEG data using the established correlation matrix. These fake EEG signals are then passed to the targeted authentication system on the user's device. The victim's authentication system then grants access to the attacker if the fake EEG samples match the stored authorized user's template.

questions regarding the content in the video for another 300 seconds. The process was repeated for the second selected video. We recorded EEG signals and hand movements throughout the entire sessions.

Inspired by the methods presented in the literature [44, 53], we designed an authentication system based on EEG signals recorded from the users. We performed a systematic analysis to study the underlying relationship as measured through Pearson correlation coefficients [7, 11] between the brainwave signals and corresponding hand movements. Our study showed that a high degree of correlation exists between brainwave signals and hand movements. Based upon the correlation model computed from a large population dataset and the hand movement data of a targeted user to be impersonated, we successfully estimated the user's EEG signals while the user was typing on the keyboard. We rigorously explored the effects of the attack, and our attack results showed an increase in the mean equal error rate (EER) of the classifiers by 180% to 36%.[1] The high mean EER values indicate that the genuine users begin to see very high false reject rates (FRRs), whereas the impostors see equally high false acceptance rates (FARs).

Our attack presents a potentially lethal security threat and negates the widely held view that it would be impossible to mimic and replicate brain activities (e.g., EEG readings) without access to the EEG device. Our assumption in the attack model is that the adversary has stolen hand movement patterns and possesses the knowledge of the correlation matrix among features of hand movement and brain patterns. We posit that this type of attack can be easily launched, as consumer-grade wearable devices have become more popular and commonplace, and can easily be compromised by installing a malicious application [26]. In addition, the correlation among features can be obtained from publicly available resources such as public datasets or works such as ours.

Our work brings forth the following contributions to the field of physiological and behavioral biometrics authentication:

(1) We present empirical evidence of the relationship between physiological biometrics stemming from the human brain (EEG) and behavioral biometrics stemming from hand movements. Our findings open up a new mode of attacks on biometric systems through exploring the intrinsic neurological or neuromuscular links among various body components.
(2) We propose a novel attack on EEG-based authentication systems by taking advantage of the correlation among the hand movements and brainwave signals to generate fake EEG signals. Our article exposes a major threat on EEG-based authentication mechanisms. An adversary who gains access to the user's hand movement patterns[2] and possesses the knowledge of correlation among the hand movements and the brainwave signals[3] poses a serious security threat.
(3) We perform a systematic analysis of features from EEG signals and corresponding hand movements. The brainwave patterns were recorded using a NeuroSky headset and an Emotiv Epoc+ headset, whereas the hand movement patterns were captured using a Sony smartwatch [45]. The data was collected from 59 users while the users watched a given video for 300 seconds and then typed on the keyboard about the content on the watched video for another 300 seconds. Feature analysis and study of any interrelation among the users' hand movements and brainwave signals show a strong correlation between the two biometric modalities.

The rest of the article is organized as follows. Section 2 discusses the related work. Section 3 presents the detailed attack model. We discuss and describe the experimental data and experimental setup in Section 4. Section 5 describes the details of the attack process on a NeuroSky-based EEG and an Emotiv-based EEG. The analysis and

[1] Later, Figure 6(e) shows the increase in mean EER from 0.026 to 0.094 with $\theta = 0.20$ and to 0.096 with $\theta = 0.23$ (i.e., an increase of approximately 355% and approximately 363%, respectively, in the mean EER) while using linear discriminant analysis (LDA)–based EEG authentication system.

[2] An adversary can steal a targeted user's hand movements by sending or installing a malicious application on the user's smartwatch device (see Liu and Sun [26]).

[3] The knowledge of correlation can be obtained using publicly available datasets or from articles such as ours.

attack performance results are presented in Section 6. We discuss the limitations of our work in Section 7. Finally, we draw our conclusions and discuss future directions for the research in Section 8.

## 2 RELATED WORK

With the increased use of wearable devices, biometric authentication has gained popularity in recent years. Biometric-based systems to authenticate the claimed identity relies on "something that you are" to distinguish between an authorized individual and an imposter. Physiological biometrics such as fingerprints and faces, despite being very popular and being widely used in today's wearable devices, suffer from several forgery issues. Researchers have proposed brainwave-based authentication systems that rely on the hidden distinctive features in EEG signals to differentiate an authorized individual from an imposter. Brainwave-based authentication systems are widely believed to be resistant to forgery attacks. This article proposes a novel correlation-based attack on EEG-based biometrics using another easily recordable biometric—hand movements.

To put our work into perspective, we discuss some of the closely related works as follows. We discuss (1) brainwave-based authentication, (2) attack models using brainwave signals, (3) hand movement–based authentication, and (4) attacks using hand movements.

### 2.1 Brainwave-Based Authentication

Research has shown that the brainwave data of an individual can be used to authenticate an individual. Brainwave-based authentication methods use the distinctive EEG signal of an individual while she or he performs a specific task [20, 21, 39]. Serwadda and Phoha [43] proposed an authentication system that uses functional near-infrared spectroscopy (fNIRS) as an authentication modality. Their method requires a user to perform simple arithmetic tasks on the computer and uses the distinctive fNIRS features to differentiate between an authorized user and an imposter. The authentication system was shown to achieve an average EER of 0.036 using a support vector machine (SVM)-based classifier and an average EER of 0.046 using a naive Bayes (NB)-based classifier on a dataset of 50 users.

Another EEG-based authentication system proposed by Ashby et al. [4] used distinctive features from a 14-channel Emotiv Epoc device while the user performed a set of three chosen mental activities for 150 seconds to authenticate an individual.

The authentication model proposed by Nakamura et al. [39] used an in-ear EEG sensor to record the user's in-ear EEG signal in the user's rest state for authentication.

The work by Liew et al. [24] introduced an incremental fuzzy-rough nearest neighbors–based authentication system. The authors showed that their model was able to authenticate the users in their dataset, comprised of 37 volunteers, using a user's EEG signals triggered using visual stimuli. The model needs a small training set to initialize and adds or eliminates the test objects for incremental training based on a threshold-based criterion on a similarity measure.

#### 2.1.1 *Comparison with Our Work.*

All of the preceding works [4, 24, 39, 43] utilize distinctive features from brainwave signals of individuals captured using EEG recording devices with one or more channels. The methods use the widely used zero-effort testing to test the performance of their authentication system. Although the model proposed by Liew et al. [24] uses the incremental training process, it does not consider the correlation between the hand movements and EEG signals and relies on zero-effort testing.

In our work, we design a correlation-based attack model and show that zero-effort testing is not sufficient for EEG-based authentication systems. We design two different authentication models using two different EEG capturing devices: (1) a neuroSky headset and (2) a 14-channel Emotiv Epoc+ device. We perform a zero-effort test and a non-zero-effort test. For the non-zero-effort test, we utilize the easily recordable hand movements of the user and the population correlation between brain waves and hand movements. The success of our attack (or the failure of our non-zero-effort test) model shows the need for a more robust test for EEG-based authentication systems against attacks such as ours.

### 2.2 Attack Models Using the Brainwave Signals

An interesting threat model was proposed by Martinovic et al. [34] that uses EEG signals to decipher the user's private information, such as credit card details, date of birth, where the user lives, knowledge of persons known to the user, pin numbers, and the user's bank details. The attack model uses an EEG gaming device such as Emotiv Epoc to form a potential attack vector to infer the secret and private information of the users. Experiments included recording the user's EEG signals while they scanned the visuals of their personal details.

*2.2.1 Comparison with Our Work.* The attack model by Martinovic et al. [34] used the EEG as an external stimulus to decipher the user's private information. In our work, we sought to predict brain activity patterns by exploiting the interrelation between hand movements and brain activities (see Section 3). We show that this predicted brain activity can be utilized to attack an EEG-based authentication system and gain access to the user's device.

### 2.3 Hand Movement–Based Authentication

With the increasing use of wearable devices such as the smartwatch, several authentication methods have been proposed by researchers that use motion sensor data captured from the user's smartwatch [12, 22, 23, 51]. The continuous authentication system proposed by Kumar et al. [23] used the distinguishing characteristics of arm movements while an individual walks. The authors showed that their model achieved a dynamic FAR and a dynamic FRR between 0% and 15% and 0% and 14.62%, respectively, using different classifiers.

Another smartwatch-based authentication system proposed by Johnston and Weiss [17] used a biometric gait recognition technique captured from the smartwatch motion data using accelerometer and gyroscope sensors. They showed that their method achieved an average authentication accuracy of greater than 92%.

Shukla et al. [46] proposed a tap-based authentication model that utilizes the unique hand movements of an individual while performing afew simple taps on the anchor points on their body. The method was shown to achieve an average accuracy of greater than 99% on a dataset of 23 subjects. A similar work by Burda et al. [8] used hand movements captured while one picks up a device from his or her pocket. The model authenticates an individual based on the unique trajectory created for the pickup action captured using motion sensors on a device. Lu et al. [29] proposed a hand gesture–based authentication system that requires an individual to draw an in-air signature to authenticate. Another closely related work is by Mayrhofer and Gellersen [35], who used unique hand movements when a user shakes a device.

*2.3.1 Comparison with Our Work.* All of these authentication models rely on zero-effort testing and do not consider any intercorrelations between hand movements and other modalities. However, our work takes another look at brainwave-based authentication systems and examines correlations between hand movements and brainwave signals that can be utilized to attack on brainwave-based authentication systems.

### 2.4 Attack Model Using Hand Movements

Sarkisyan et al. [42] proposed an attack on a user's pin using the motion sensor data from the user's smartwatch. The attack relies on a malware that either the user installs on his or her smartwatch or is installed by the attacker on the user's smartwatch. The malware reads the user's hand movements and sends the data to a remote server using the paired smartphone. Other works by Wang et al. [53] and Maiti et al. [31, 32] show a hand movement–based attack on the text typed by the user on his or her laptop or desktop keyboard. Based on the observed accelerometer and gyroscope readings of the user's hand, the attack model computes the distance traveled and the rotation of the user's hand. The authors show that their attack was able to successfully decipher the words and sentences typed by the user by using motion signals with a language-based dictionary model for English language words and sentences.

The work of Beltramelli and Risi [5] shows an attack model on touch-logging and key-logging on handheld devices such as smartphones. The attack model uses the hand movement data captured using a smartwatch or wristband with built-in motion sensors. The authors show that deep learning algorithms such as LSTM can learn the user's hand movement patterns and successfully decipher the text typed on touchscreen devices.

*2.4.1 Comparison with Our Work.* The hand movement–based attack models discussed earlier use motion signal data from a smartwatch or smart wristband to attack on the user's typing, such as the pin, passwords, or the typed text. In our work, we use the user's hand movements and the population-based interrelations between the user's hand movements and his or her brainwave signals to build an attack on the EEG-based authentication system.

## 3 ATTACK MODEL: GENERATING SPOOFED EEG SIGNALS

This section presents the attack model on EEG-based authentication systems. The attack utilizes the knowledge of correlations between the users' hand movements and their brainwave activities. Given a user's hand movement data, our attack model can successfully decipher the corresponding brainwave signals using the correlation model between the two signals previously learned from population data. Figure 2 shows the workflow of our attack model. The hand movements were captured using a Sony smartwatch, and the brainwave signals were recorded using a NeuroSky headset or an Emotiv Epoc+ headset. The attacker possesses knowledge of the correlation between the two signals and steals the victim's hand movement patterns while he or she types on the keyboard. The adversary then utilizes the previously learned correlations and stolen hand movement patterns to generate the victim's brainwave patterns (i.e., fake EEG signals). The attacker uses the generated fake EEG signals to gain access to the user's device, which is secured through an EEG-based authentication system.

**ALGORITHM 1:** Attack Model on an EEG-Based Authentication System.

```
Input: EEG features, $\boldsymbol{A}$, Smartwatch features $\boldsymbol{S}$, Threshold $\theta$.
Output: Mimicked EEG features $\boldsymbol{A}^{\boldsymbol{mimic}}$
Construct pairwise correlation matrix $r_{AS}$ using $\boldsymbol{A}$ and $\boldsymbol{S}$.
Select $\boldsymbol{A}^{C}$ and $\boldsymbol{S}^{C}$ using Equation (1).
Estimate EEG features $\boldsymbol{A}^{\boldsymbol{Cest}}$ based on linear regression model in Equation (2).
Generate the mimicked EEG features $\boldsymbol{A}^{\boldsymbol{mimic}}$ using $\boldsymbol{A}^{\boldsymbol{Cest}}$ and $\boldsymbol{A}^{\boldsymbol{Dummy}}$.
```

Our attack model is easy to launch, as it only requires the user's hand movement patterns to attack the targeted authentication systems. As shown in several prior studies [14, 28, 38, 52], Bluetooth- or WiFi-enabled wearable devices (e.g., smartwatches and wristbands) have become the targets of attacks, and various personal private information (e.g., motion data) has suffered from the increasing risks of leakage and disclosure. In this study, it is assumed that the attacker can gain access to the legitimate user's hand movement patterns by compromising the user's wearable devices. For instance, this could be done by sending or installing a malicious application in the user's device.

Let the features of hand movement patterns collected from a smartwatch be $\boldsymbol{S} = \{\boldsymbol{S}_1, \boldsymbol{S}_2, \ldots \boldsymbol{S}_{\boldsymbol{m}}\}$ and the brain activity patterns collected from a wearable EEG device be $\boldsymbol{A} = \{\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_{\boldsymbol{n}}\}$, where $\boldsymbol{S}_{\boldsymbol{j}}$ and $\boldsymbol{A}_{\boldsymbol{i}}$ are the $j$th and $i$th feature of $\boldsymbol{S}$ and $\boldsymbol{A}$, respectively. Both $\boldsymbol{S}_{\boldsymbol{j}}$ and $\boldsymbol{A}_{\boldsymbol{i}}$ are time series data. Let $\boldsymbol{r}_{\boldsymbol{AS}}$ be the correlation matrix between $\boldsymbol{A}$ and $\boldsymbol{S}$. The correlated subset of $\boldsymbol{A}^{C}$ and $\boldsymbol{S}^{C}$ are shown in Equation (1), where $\theta$ is a user-defined parameter:

$$\boldsymbol{A}^{C} \subset \boldsymbol{A} \mid \boldsymbol{r}_{\boldsymbol{AS}} > \theta,\ \boldsymbol{S}^{C} \subset \boldsymbol{S} \mid \boldsymbol{r}_{\boldsymbol{AS}} > \theta. \tag{1}$$

Let $A^{mimic}$ be a feature set of brain activities. The adversary estimates $A^{mimic}$ by $A^{mimic} = \mathbb{F}(S^{C})$. We propose a way of representing $F(.)$ using an equation of linear regression with standardized data variables [19] as described by $A^{Cest}_{std} = r^{pop}_{A^{C}S^{C}} * S^{C}_{std}$. The correlation coefficient between the correlated features of brain activities and hand movement patterns from the population is $r^{pop}_{A^{C}S^{C}}$. The standardized variables $A^{Cest}_{std}$ and $S^{C}_{std}$ are defined as follows [19]:

$$A^{Cest}_{std} = \frac{A^{Cest} - \bar{A}^{Cpop}}{\sigma^{pop}}; \; S^{Cattc}_{std} = \frac{S^{Cattc} - \bar{S}^{Cattc}}{\sigma^{attc}}. \tag{2}$$

The attacker estimates $A^{Cest}$ using stolen hand movement features $S^{Cattc}$ of a legitimate user. $\bar{S}^{Cattc}$ and $\sigma^{Cattc}$ are the mean and standard deviation of hand movement patterns of the *attacker*, respectively. The threat model uses the *population* mean $\bar{A}^{Cpop}$ and the standard deviation of brain activity patterns $\sigma^{pop}$ to standardize $A^{Cest}$. The threat model thus estimates and synthesizes the counterfeit features of brain activities using Equation (3):

$$A^{Cest} = \left\{ r^{pop}_{A^{C}S^{C}} * \sigma^{pop} * \frac{S^{Cattc} - \bar{S}^{Cattc}}{\sigma^{attc}} \right\} + \bar{A}^{Cpop}. \tag{3}$$

Generally, it was observed that $|A^{C}| \subset |A|$. Therefore, we filled the empty feature positions $A^{Dummy}$ with the randomly selected, least correlated features from any of the users excluding the user who was currently selected for the attack. Finally, the fake EEG feature data was generated by $A^{mimic} = \{A^{Cest} \cup A^{Dummy}\}$ to attack the targeted authentication system. The detailed procedure of the attack model is described in Algorithm 1.

## 4 DATA COLLECTION EXPERIMENTS

With the approval of our university's institutional review board (IRB), we recruited a total of 59 volunteer participants using an email invitation to the departments' listserv at our university. Volunteer recruitment was done in two different phases. Phase I data collection had 32 volunteer participants, where we used a NeuroSky headset to record EEG data. We recruited 27 different volunteer participants in phase II of data collection, where an Emotiv Epoc+ headset was used for EEG data recording. We call phase I data as *NeuroSky-based data* and phase II data *Emotiv-based data* in the rest of the article. We obtained the informed written consent from all participants for using the collected data for this specific research. The participation in our study was voluntary, and the participants were briefed about the data collection procedure and the research question before the start of the data collection experiments. All participants were students, staf,f or faculty, between 20 and 32 years of age, in the department of electrical engineering and computer science at our university.

Each participant provided data in two different sessions: a training session and a testing session. Each session was divided into four different types of activities (Table 1):

(1) *Watch the First Video (Video I)*: The participant watched the first assigned video on the computer screen for 300 seconds. The rest of the video was discarded.
(2) *Type on the Keyboard (Video I)*: The participant typed his or her responses to the previously designed questions about the story played in the video. The typing activity was restricted to 300 seconds.
(3) *Watch the Second Video (Video II)*: The participant watched the second assigned video on the computer screen for 300 seconds. The rest of the video was discarded.
(4) *Type on the Keyboard (Video II)*: The participant typed his or her responses to the previously designed questions about the story played in the video.

There was a rest period of 3 to 4 minutes between any two consecutive activities. We recorded the participants' hand movements through the motion sensors (i.e., accelerometer and gyroscope) available within the smartwatch and the brainwave activities through the wearable EEG headset.

Table 1. List of Activities Performed by the Participants in Each Data Collection Session

| **Start Session: Place the EEG headset (NeuroSky or Emotiv Epoc+) on the User's Head and the Smartwatch on the Hand** | | | |
|---|---|---|---|
| Video | Action | Devices | Sensors |
| I | Watch (300 seconds) | Smartwatch | Accelerometer, Gyroscope |
| | | EEG headset | EEG |
| | Respond (300 seconds) | Smartwatch | Accelerometer, Gyroscope |
| | | EEG headset | EEG |
| **Rest (60 Seconds)** | | | |
| II | Watch (300 seconds) | Smartwatch | Accelerometer, Gyroscope |
| | | EEG headset | EEG |
| | Respond (300 seconds) | Smartwatch | Accelerometer, Gyroscope |
| | | EEG headset | EEG |
| End session: Remove the EEG headset from the user's head and the smartwatch from the hand. | | | |

*Note:* Video 1 was randomly selected from a pool of short videos containing happy emotional content, whereas a randomly selected Video 2 contained sad emotional content. All four activities' data was recorded for 300 seconds each (1,200 seconds of total data for a session), and the same activities were repeated for a second session (testing) of data collection where a different set of videos was selected from the video pool (see Appendix A).

We selected a pool of 40 videos from a video networking website (see Appendix A for the list of selected videos) and randomly assigned four different videos from the pool of videos to each participant in our study: two videos for the training session and the other two videos for the testing session. For each session, the first video was selected from the pool of videos with happy emotional content, and the other video was drawn from the pool of videos with sad emotional content. There was an average gap of 5 to 6 days between the two sessions' data.

The questions in the typing exercises were general and repeated for all the videos: (1) How do you feel about the video? (2) What type of emotion are you getting after watching this video? (3) Can you give a summary of the video content?

Each recorded session was preceded with a practice session lasting between 2 and 3 minutes to help the participants become familiar with the experimental procedures and devices. The recorded session followed the practice session, ensuring that the participants felt familiar and comfortable with all experimental settings.

### 4.1 NeuroSky-Based Data

We recruited 32 volunteer participants (26 male and 6 female) for our NeuroSky-based data collection. Each volunteer was invited for two different sessions on two different days. Each participant wore a Sony smartwatch on the wrist[4] to capture hand movements and a NeuroSky headset to record EEG signals. We developed an Android application on a smartphone paired with both the smartwatch and the NeuroSky headset to record these signals in a time-synchronized manner. The sampling rate of the NeuroSky headset was set to 512 Hz, and the sampling rate for accelerometer and gyroscope sensors were set to 80 Hz. To avoid the loss of the data due to interrupts in the smartwatch and the smartphone, we buffered the data for 5 seconds in the smartwatch using Android Wear and then transferred them to the smartphone.

For each session, the Sony smartwatch and the NeuroSky headset were reset and paired appropriately.

### 4.2 Emotiv-Based Data

We recruited 27 volunteer participants (22 male and 5 female) for our Emotiv-based data collection. Each volunteer was invited for two different sessions on two different days. Each user wore a Sony smartwatch on the left wrist and another Sony smartwatch on the right wrist to record hands movements. The participants wore an Emotiv Epoc+ headset to record their EEG signals. We developed a Java-based application to connect and transfer the collected data from the smartwatches via Bluetooth to the desktop or laptop. For the Emotiv Epoc+ device, we used EmotivPro software. The sampling rate of the Emotiv Epoc+ headset was set to 128 Hz, and the accelerometer and gyroscope sensors in the Sony smartwatch recorded the data with a sampling frequency of 80 Hz.

For each session, both the Sony smartwatches and the Emotiv Epoc+ headset were reset and paired appropriately.

## 5 ATTACK DETAILS

We used two different EEG recording devices to implement and validate our attack model: (1) a very simple NeuroSky headset and (2) a 14-channel Emotiv Epoc+ headset. NeuroSky-based EEG attack enabled us to verify existence of correlation between the hand movements and the EEG data with limited channels. However, the Emotiv-based EEG analysis enabled us to validate the existence of correlation and applicability of our attack model on a more sophisticated EEG-based authentication system designed using 14-channel EEG signals.

We recorded hand movement signals and brainwave signals simultaneously while the users typed on a laptop or were asked to watch a given video with some emotional content. We divided our analysis into two phases: (1) NeuroSky-based analysis and (2) Emotiv-based analysis.

In NeuroSky-based analysis, we validated the correlations and applicability of our attack with hand movement data where the user wore a smartwatch in one of their hands.[5]

In Emotiv-based EEG analysis, we recorded hand movement data from both hands of the user. We provided two smartwatches to the participants, one for each hand. This enabled us to address the question of whether or not existence of correlation between hand movements and the EEG signal has any dependence on a particular hand of the user. To address this, we implemented our attack using the population correlations and snooped hand movement data captured from the left hand of the participants. The attack was repeated where implementation was done using the right hand movements and a comparative analysis of both attack implementations was performed.

The rest of this section is organized as follows. We discuss the attack implementation on the NeuroSky-based EEG in Section 5.1, and Section 5.2 describes the attack implementation details on Emotiv-based EEG signals.

[4] We did not provide any instructions to the participants regarding on which hand to wear the smartwatch. The participants chose to wear the smartwatch in the hand they normally choose or would normally wear one on. That being mentioned, the majority of participants in our experiments chose to wear the watch in their nondominant hand.

[5] We provided a smartwatch to the participants and asked them to wear it on their wrist. We did not provide any instruction regarding which wrist they needed to wear the given smartwatch. That said, the majority of participants in our dataset chose to wear the smartwatch on their nondominant hand.

## 5.1 Attack on the NeuroSky-Based EEG Signals

In this section, we present the analysis on our phase I data, NeuroSky-based data, which was collected using a NeuroSky headset and a Sony smartwatch (see Section 4). We first discuss the feature extraction framework (see Section 5.1.1) from EEG data and hand movement data. Section 5.1.2 describes the targeted EEG-based authentication system design. We discuss correlation analysis between the EEG signal and hand movement signals in Section 5.1.3.

*5.1.1 Data Preprocessing and Feature Extraction.* The preprocessing is performed using the following three steps for both the NeuroSky and smartwatch data:

(1) First, we checked the error values in the NeuroSky data. NeuroSky provided the signal quality parameter while sending the data to the smartphone. If the signal quality attribute value was zero, then it was good and the data item was accepted as valid. A higher signal quality value would indicate a less trustable and lower-quality signal recording. The signal quality parameter ranged from 0 to 250. In our experiments, we set a threshold as 200 for the signal quality values.[6] In other words, if the recorded signal quality value was more than 200, we discarded the corresponding EEG data item as invalid.

(2) In the second step, the smartwatch data was checked for missing values. We ran scripts on each user's data to check for missing values based on the timestamp information and the designated sampling rate. If the missing values were less than 20 samples, we took the average of values before and after the missing samples. We discarded the data that had more than 20 missing samples and repeated the data collection for that user.

(3) Finally, the sensory data from the NeuroSky headset and the Sony smartwatch motion sensors (accelerometer and gyroscope) was checked for synchronization errors using the timestamps of the smartphone, smartwatch, and headset. The synchronized data was stored for the following feature extraction and analysis phase.

*Feature extraction for EEG data.* We used the discrete wavelet transform (DWT) to analyze the EEG data [48] (please refer to Appendix B for details about DWT). We chose the number of decomposition levels to be 10 for our analysis. Therefore, the EEG signals were decomposed into details $H1$–$H10$ and one final approximation, $L10$. Prior literature [48] suggested that the smoothing feature of the Daubechies wavelet of order 4 (db4) makes it more appropriate to detect changes of EEG signals. Thus, we adopted the same strategy in our processing and analysis. The extracted wavelet coefficients provide a compact representation of energy distribution of the signals in time and frequency.

To reduce the dimensionality of the extracted feature vectors, the statistical features were used to represent the time-frequency distribution of EEG signals [18]. We extracted features from $H3$–$H10$, and $L10$ sub-bands. The following features were calculated for each sub-band: (1) mean of the absolute values, (2) average power, and (3) standard deviation (features 1–27, i.e., a total of 27 features from nine sub-bands). We also calculated (4) the ratio of absolute mean values for adjacent bands (features 28–35, i.e., a total of eight features from nine adjacent sub-bands).

The distribution of the signals in the frequency domain was captured by means of the absolute values and the average power computed for each sub-band. The standard deviation and the ratio of absolute mean values captured the amount of change in frequency distribution of the signals. The 36th feature represents the spectral entropy of the signals [16].

*Feature extraction for motion data.* The accelerometer and gyroscope sensors provide X-axis, Y-axis, and Z-axis motion values. For the accelerometer, each component of the acceleration is defined as $S_{ac_x}$, $S_{ac_y}$, $S_{ac_z}$, and

[6] We chose a threshold of 200 for excluding data with poor signal quality based on the manufacturer's manual for the measure of SIGNAL QUALITY [1].

Table 2. Description of 32 and 28 Features Respectively Extracted from the Accelerometer and Gyroscope

| **Smartwatch** | | | |
|---|---|---|---|
| **Feature No.** | **Accelerometer** (32 Features) | **Feature No.** | **Gyroscope** (28 Features) |
| *For each signal in* $S_{ac_x} - S_{ac_m}$ | | *For each signal in* $S_{gy_x} - S_{gy_m}$ | |
| 37–40 | Average peak interval | 69–72 | Average peak interval |
| 41–44 | Signal band power | 73–76 | Signal band power |
| 45–48 | Signal energy | 77–80 | Signal energy |
| 49–52 | Median of the magnitude | 81–84 | Median of the magnitude |
| 53–56 | No. of signal peak | 85–88 | Range of signal amplitude |
| 57–60 | Range of signal amplitude | 89–92 | Median frequency |
| 61–64 | *Median frequency that divides a power spectrum into two regions with equal amplitude* | | |
| 65–68 | Spectral entropy | 93–96 | Spectral entropy |

each component of the rotation is defined as $S_{gy_x}$, $S_{gy_y}$, $S_{gy_z}$. Using these values, we generated the magnitude of acceleration as $S_{ac_m}$ and the magnitude of rotation as $S_{gy_m}$. $S_{ac_m}$ and $S_{gy_m}$ are as expressed in Equation (4):

$$S_{ac_m} = \sqrt{S_{ac_x}^2 + S_{ac_y}^2 + S_{ac_z}^2}$$

and

$$S_{gy_m} = \sqrt{S_{gy_x}^2 + S_{gy_y}^2 + S_{gy_z}^2}. \tag{4}$$

By using four components (three axes and magnitude) of the accelerator and gyroscope data, we extracted 60 different features [23] as described in Table 2.

*5.1.2 Targeted Authentication System Prototype.* Using the 36 features extracted from EEG data, we trained an authentication classifier framework (as shown in Figure 3). The labeled training sessions' data of all users were given as the inputs to the training module, whereas the labeled testing sessions' data from all users were given as the inputs to the testing module. The framework calculated the accuracy and EER values. The mean EER values for 32 subjects using linear discriminant analysis (LDA), random forest (RF), neural network (NNet), and SVM are shown later in Figure 6(e). We obtained an average EER of 3.6% using the LDA classifier and an average EER of 3% using the NNet classifier, which represent the best performance achieved on our test data.

Another factor we are interested in investigating is the effects of variations of the time window sizes on the proposed EEG-based authentication system. We divided the entire data from 32 subjects into various sizes of time windows and performed authentication tests based on these varying time windows. Here, the $T_1$ seconds time window means that we first used $T_1$ seconds of all eight activities' data (four for training and the other four for testing) and studied how the authentication system performed during this period of time. Likewise for $T_2$ seconds, we used the first $T_2$ seconds' time of all activities. The performance (i.e., the mean EER value of 32 users) using the data with varying time windows on LDA, RF, NNet, and SVM classifiers are shown in Figure 4. It is observed that the mean EER values with LDA, RF, and NNet classifiers are quite low and the classifier model performs well to authenticate users based on their EEG brainwave signals.

*5.1.3 Details of Correlation Analysis.* Next, we seek to explore the relationships between human typing patterns and brainwave activities. We computed the correlations [6, 11] between the extracted features of the EEG headset and smartwatch data. We plotted the heatmaps of these values in Figure 5(c). The heatmaps of the correla-

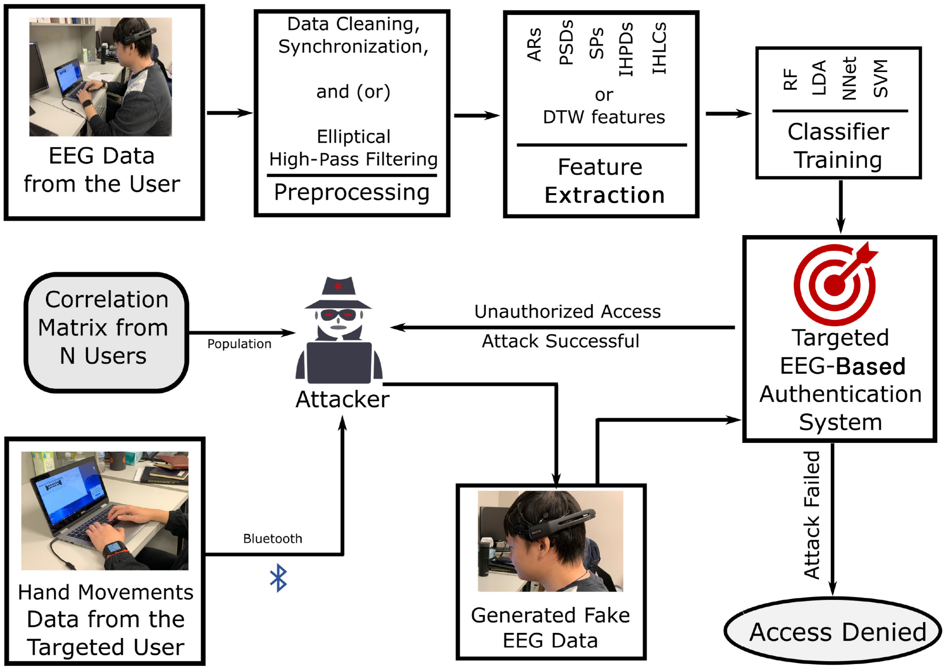


Fig. 3. Experimental protocols. EEG signals were collected using a NeuroSky headset and an Emotiv Epoc+ headset. Hand movement patterns were recorded using Sony smartwatch motion sensors. After data acquisition, the data preprocessing, feature extraction, and classifier training were performed on EEG data. A correlation matrix was computed using the training dataset from the hand movements and brainwave signals. This correlation matrix was then exploited together with the snooped hand movements of the targeted user to generate fake EEG signals. The generated fake EEG data was used to attack the user's EEG-based authentication system.

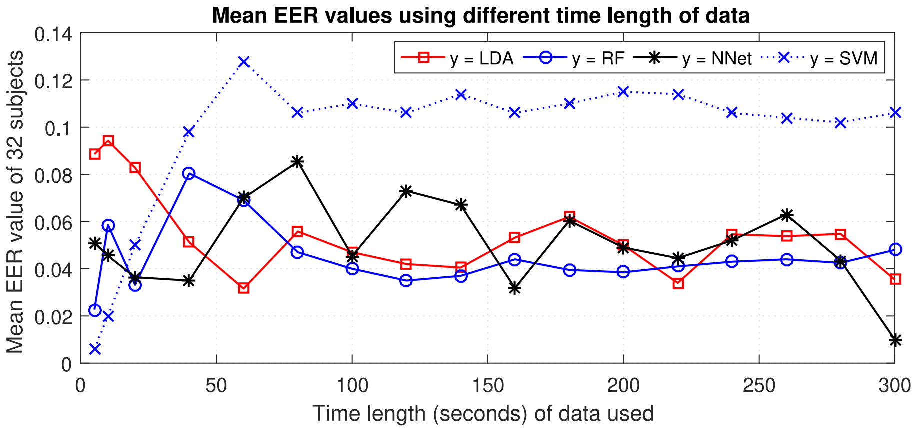
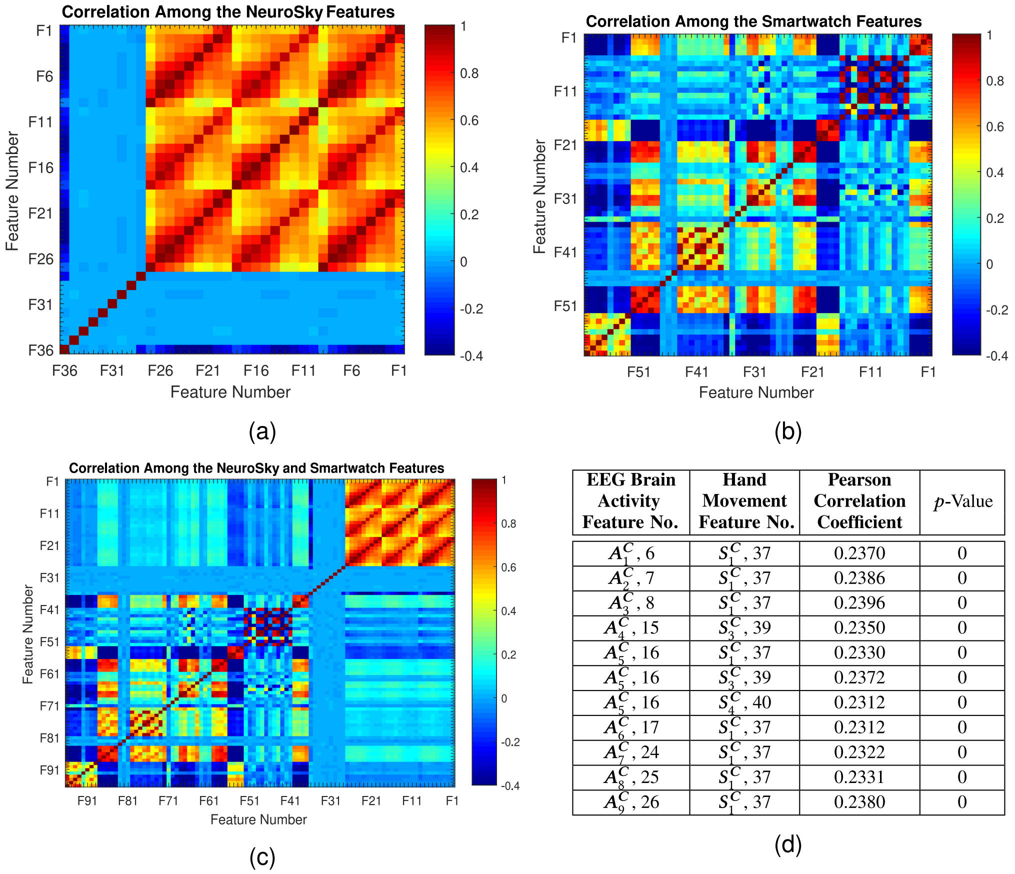


Fig. 4. Performance (mean EER value of 32 users) of the EEG-based authentication system during different time lengths of activities using four classifiers.



(a)

(b)

(c)

| EEG Brain Activity Feature No. | Hand Movement Feature No. | Pearson Correlation Coefficient | *p*-Value |
|---|---|---|---|
| $A_1^C$, 6 | $S_1^C$, 37 | 0.2370 | 0 |
| $A_2^C$, 7 | $S_1^C$, 37 | 0.2386 | 0 |
| $A_3^C$, 8 | $S_1^C$, 37 | 0.2396 | 0 |
| $A_4^C$, 15 | $S_3^C$, 39 | 0.2350 | 0 |
| $A_5^C$, 16 | $S_1^C$, 37 | 0.2330 | 0 |
| $A_5^C$, 16 | $S_3^C$, 39 | 0.2372 | 0 |
| $A_5^C$, 16 | $S_4^C$, 40 | 0.2312 | 0 |
| $A_6^C$, 17 | $S_1^C$, 37 | 0.2312 | 0 |
| $A_7^C$, 24 | $S_1^C$, 37 | 0.2322 | 0 |
| $A_8^C$, 25 | $S_1^C$, 37 | 0.2331 | 0 |
| $A_9^C$, 26 | $S_1^C$, 37 | 0.2380 | 0 |

(d)

Fig. 5. Heatmap of the correlation coefficients computed among the extracted features of a single-channel EEG signal from the headset (b), accelerometer and gyroscope sensors of the smartwatch (b), those between all features of the two devices (c), and the correlation coefficient between the feature pairs extracted from NeuroSky and smartwatch above a threshold value $\theta = 0.23$ (d).

tion coefficients computed among the brain activities and hand typing patterns features are shown in Figure 5(a) and (b), respectively. It is observed from Figure 5(b) that a rather high level of correlation exists among the features of hand motion data. This is obvious given the fact that these motion sensors basically record the hand movements of the subjects. It is also observed from Figure 5(a) that there is a high degree of correlation among the features of EEG brainwave data. This is due to the existence of correlations among the features extracted from the different sub-bands of EEG data using DWT.

More interestingly, it is found that a significant level of correlation exists among the features of the EEG data and the accelerometer/gyroscope data. This observation can be seen in the upper left half of Figure 5(c). The exact values between some features of the cross platforms are listed in Figure 5(d).

## 5.2 Attack on the Emotiv-Based EEG Signals

In this section, we present the analysis on our phase II data, Emotiv-based data, which was collected using an Emotiv Epoc+ headset and two Sony smartwatches (see Section 4). We first discuss the feature extraction framework (see Section 5.2.1) from EEG data, as well as hand movement data. Section 5.2.2 describes the targeted

Emotiv EEG-based authentication system design, and we discuss correlation analysis between Emotiv-based EEG signals and hand movements in Section 5.2.3.

### 5.2.1 *Data Preprocessing and Feature Analysis.*

In this section, we first discuss feature extraction from Emotiv-based EEG data. We follow the feature extraction on EEG signal with details of the feature extraction process from the hand movement data.

*Feature extraction from Emotiv EEG data.* A window of 2.5 seconds was used with an overlap of 1.5 seconds for feature extraction. Each 2.5 second long data segment was high-pass filtered with a second-order 2-Hz cut-off elliptic filter. We ensured no phase distortion by applying forward and reverse filtering. We extracted a total of 2,688 features from each of the overlapping data segments. Brief details of the extracted features include the following:

(1) *Autoregressive coefficients*: An autoregressive (AR) model of the sixth order was used on high-pass filtered data, which gave us six AR coefficients for each electrode resulting in a total of 84 features, $AR_1, \ldots, AR_{84}$:

$$x(n) = \sum_{k=1}^{M} a_k x(n-k) + e(n),$$

where $M$ is the order of the AR model, $x(n)$ is the signal value at the sampled point $n$, $a_k$ are the real valued AR coefficients, and $e(n)$ is an independent error term.

(2) *Power spectral density*: The square of the absolute value of the Fourier transform for each data segment gave us the power spectral density (PSD), consisting of 160 points for each of the electrodes. This resulted in a total of 2,240 PSD features, $PSD_1, \ldots, PSD_{2240}$.

(3) *Spectral power*: The spectral power (SP) was computed in five frequency bands: delta (0–4 Hz), theta (4–7 Hz), alpha (8–13 Hz), beta (14–20 Hz), and gamma (21–50 Hz) for each electrode. SP was obtained by integrating the computed spectral density over the preceding five frequency bands. This resulted in a total of 70 SP features (5 SPs per electrode), $SP_1, \ldots, SP_{70}$.

(4) *Interhemispheric power difference*: Interhemispheric power differences (IHPDs) were computed for each of the five frequency bands between each pair of electrodes in the left and right hemispheres as follows:

$$IHPower_{diff} = (P_1 - P_2)/(P_1 + P_2),$$

where $P_1$ and $P_2$ are the powers of two different electrodes in the same spectral band and in the opposite hemisphere. This gave us 49 different combinations (seven electrodes in each hemisphere) for each of five frequency bands, resulting in a total of 245 IHPD features, $IHPD_1, \ldots, IHPD_{245}$.

(5) *Interhemispheric channel linear complexity*: Interhemispheric channel linear complexity (IHLC) is a measure of spatial synchronization of the data. For a certain $C$ number of channels ($C$-channel) signals, IHLC can be defined as follows:

$$\Omega = \exp\left(\sum_{i=1}^{C} \zeta_i \log \zeta_i\right)$$

$$\zeta_i = \frac{\lambda_i}{\sum_{i=1}^{C} \lambda_i},$$

where$\lambda_i$ are the eigenvalues of the covariance of the $C$-channel EEG matrix and $\zeta_i$ are the normalized values of $\lambda_i$. $\Omega$ represents the IHLC values. A high value of $\Omega$ indicates a low correlation between the signals of the electrodes and vice versa. A total of 49 IHLC features, $IHLC_1, \ldots IHLC_{49}$, were computed for all possible electrode combinations among the two hemispheres.

*Feature extraction from motion sensor data.* By using four components (three axes and magnitude) of the accelerator and gyroscope data, we extracted 60 different features from the motion sensor data collected from the

Table 3. Hand Movements and Emotiv EEG Feature Pairs and the Corresponding Pearson Correlation Coefficients Obtained Using Our Training Dataset

| Emotiv EEG Signal Feature No. | Hand Movement Feature No. | Pearson Correlation for the Left Hand | Pearson Correlation for the Right Hand |
|---|---|---|---|
| $AR^{C}{}_{52}$, 52 | $S^{C}{}_{8}$, 44 | 0.2471 | 0.2388 |
| $AR^{C}{}_{52}$, 52 | $S^{C}{}_{8}$, 44 | 0.2315 | 0.2164 |
| $PSD^{C}{}_{8}$, 92 | $S^{C}{}_{12}$, 48 | 0.2265 | 0.2563 |
| $PSD^{C}{}_{40}$, 124 | $S^{C}{}_{32}$, 68 | 0.2463 | 0.2385 |
| $SP^{C}{}_{5}$, 2329 | $S^{C}{}_{32}$, 68 | 0.2453 | 0.2014 |
| $SP^{C}{}_{6}8$, 2340 | $S^{C}{}_{32}$, 68 | 0.2517 | 0.1895 |
| $IHPD^{C}{}_{32}$, 2426 | $S^{C}{}_{44}$, 80 | 0.1989 | 0.2157 |
| $IHPD^{C}{}_{245}$, 2639 | $S^{C}{}_{44}$, 80 | 0.2483 | 0.2365 |
| $IHLC^{C}{}_{2}$, 2641 | $S^{C}{}_{44}$, 80 | 0.2261 | 0.2332 |
| $IHLC^{C}{}_{40}$, 2679 | $S^{C}{}_{59}$, 95 | 0.1879 | 0.2159 |
| $IHLC^{C}{}_{45}$, 2684 | $S^{C}{}_{59}$, 95 | 0.2364 | 0.2458 |

smartwatch that the users wore in their right hand. The feature details are described in Table 2, and the process is the same as discussed in Section 5.1.1.

The feature extraction process was repeated for the motion sensor data recorded from the smartwatch that the users wore in their left hand.

*5.2.2 Emotiv EEG-Based Authentication System.* Using all 2,688 features for Emotiv EEG data, we trained five—LDA, RF, NNet, and —to authenticate a user. We used the session I Emotiv EEG dataset to train our Emotiv EEG–based authentication system for each user. For each user, we supplied session I data from the user as genuine samples and randomly selected samples from session I data of the rest of the users as imposter samples for training the authentication model. We tested the performance of our Emotiv EEG–based authentication system using session II data, where we constructed genuine and imposter samples with same approach as used for training samples.

We calculated the accuracy and EER values. The mean EER values for 27 subjects using LDA, RF, NNet, and SVM are shown later in Figure 10(e). We obtained an average EER of 5.8% using the LDA classifier, 6.3% using the RF classifier, an average EER of 6.8% using the NNet classifier, and an average EER of 8.6% using the SVM classifier.

*5.2.3 Analysis of Correlations Between Emotiv EEG and Hand Movements.* To explore the relationships between the user's hands movement patterns and brainwave activities, Pearson correlations [6, 11] were computed between the extracted features of Emotiv EEG data and the users' right hand smartwatch features. We also computed the correlations between the extracted features of Emotiv EEG data and the users' left hand smartwatch features. Pearson correlation analysis confirmed the existence of correlations among the features of hand motion data of either hands and Emotiv-based EEG features. Pearson correlation coefficients for some features pairs are shown in Table 3. Based on the correlation coefficients obtained in this step, we used hand movement data from the test session and generated fake EEG samples corresponding to each hand movement feature vector (see Section 3).

## 6 ATTACK PERFORMANCE EVALUATION

In this section, we first discuss the performance of our attack on the authentication system that uses NeuroSky-based EEG signals in Section 6.1. The attack performance on the Emotiv-based EEG authentication system is discussed in Section 6.2.

## 6.1 Attack Performance on NeuroSky-Based EEG

In this section, we evaluated the performance of the proposed attack model on the EEG-based authentication system, leveraging the underlying correlation between the hand movements and EEG brain waves. We used the generated fake EEG data (see Section 3) to attack the legitimate users in the designed targeted authentication system. To this aim, we first trained the model with the training session's data of a legitimate user. For testing, we considered that the attacker had access to the legitimate user's hand movement data, which is $\boldsymbol{S^{attc}}$. The user's brain activity data was synthesized and mimicked using Algorithm 1. Thus, a fake user profile $\boldsymbol{U^{faked}}$ was created by merging these two sets of features—that is, $\boldsymbol{U^{faked}} = \{\boldsymbol{A^{mimic}} \cup \boldsymbol{S^{attc}}\}$, which was used for attack.

*6.1.1 Attack Performance for Each User.* We repeated this experiment for each user in our study with varying values of $\theta$ as 0.20 and 0.23. Figure 6 shows the attack performance on each user in our study for four different classification algorithms used to build the EEG-based authentication systems. Figure 6(e) shows the overall mean EER values computed for all users in our study. It is observed from Figure 6(e) that there are significant increases in EER values with attack. This observation is valid for different $\theta$ values and for all classifiers.

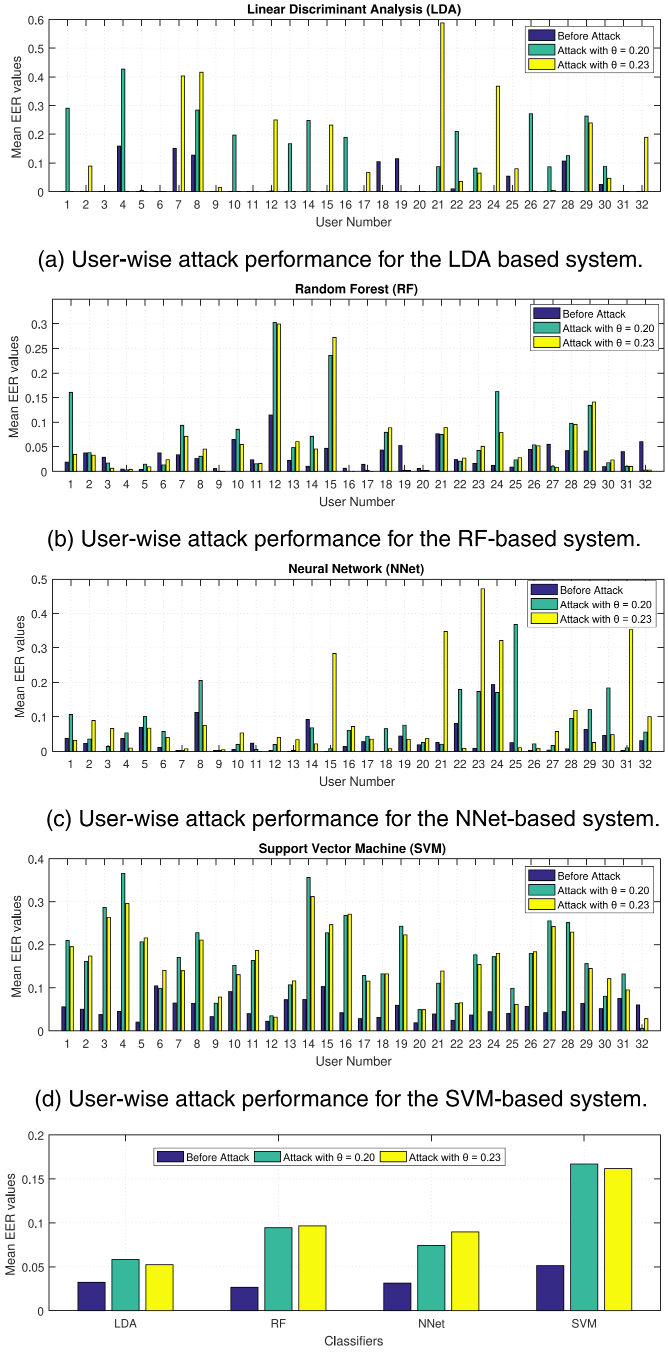
*6.1.2 Attack Performance for Decision Time.* We then analyzed the effects of the variations of time window lengths of activities on the proposed attack model. We divided the time segments with the same procedure as we did in the case of testing the authentication model. The result is presented in Figure 7, where the subscript *after* represents the values with the proposed snoop-forge-replay attack. The mean EER value increases by 4% with LDA, 3% with RF, 6% with NNet, and 14% with SVM classifiers based upon the generated attack data. It can be observed that the attack cases have higher mean EER values than the cases when the attack was not deployed (subscript *before*) in all time segments with all classifiers.

*6.1.3 Attack Performance for the Time Interval Between User Registration and Attack.* We further analyzed the effects of variations of time intervals between registering the user into the system and launching the proposed attack. To this aim, we performed the attack on the users with three different time interval windows between the user registration and attack: (1) less than 3 days, (2) more than 3 days but less than 7 days, and (3) more than 7 days but less than 11 days. We collected the genuine users' samples on the day when the attack was launched and compared the performance of the attack against the genuine user authentication performance. As shown in Figure 8, it is observed that the attack cases (green with $\theta = 0.20$ and yellow with $\theta = 0.23$) have higher mean EER values than the cases when the attack was not deployed (blue).

*6.1.4 Attack Performance with Users' Gender.* We also analyzed the effects of the users' gender on the performance of the attack. As shown in Figure 9, our results show that the attack was generally successful for both female and male subjects, and the attack cases (green with $\theta = 0.20$ and yellow with $\theta = 0.23$) have higher mean EER values than the cases when the attack was not deployed (blue). There was an exception in the case of female users with an RF-based EEG authentication system. We believe that this behavior could be an outlier, given the fact that we have a relatively small number of female subjects (i.e., 6 female and 26 male) in our dataset.

## 6.2 Attack Performance on Emotiv-Based EEG

By leveraging the correlation obtained in Section 5.2.3 and the hand motion feature values from the test session, we generated the corresponding Emotiv EEG feature, $Fake_{EEG}$, as the attack data for each user (see Section 3). To test the performance of our attack, we supplied generated $Fake_{EEG}$ feature vectors as the test sample to our Emotiv EEG-based authentication system. We computed the EERs for the authentication system based on each of RF, LDA, NNet, and SVM classifiers. We present the performance of the attack using $Fake_{EEG}$ samples for each user and the attack performance with gender as follows.



(a) User-wise attack performance for the LDA based system.

(b) User-wise attack performance for the RF-based system.

(c) User-wise attack performance for the NNet-based system.

(d) User-wise attack performance for the SVM-based system.

(e) Classifier-wise mean EER computed over all users.

Fig. 6. Mean EER values before and after user-specific attack for LDA (a), RF (b), NNet (c), and SVM (d), and the mean EER before and after attack computed over all users (e). Attack performance is shown with varying thresholds of $\theta = 0.20$ (green) and $\theta = 0.23$ (yellow).

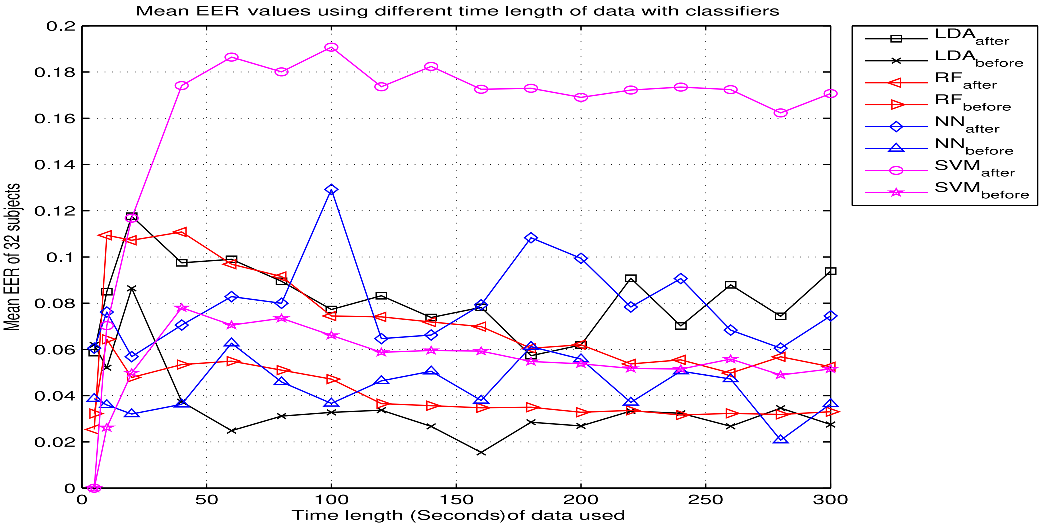


Fig. 7. Performance of the proposed attack model using different time window length of all activities with LDA, RF, NNet, and SVM verifiers ($\theta = 0.23$).

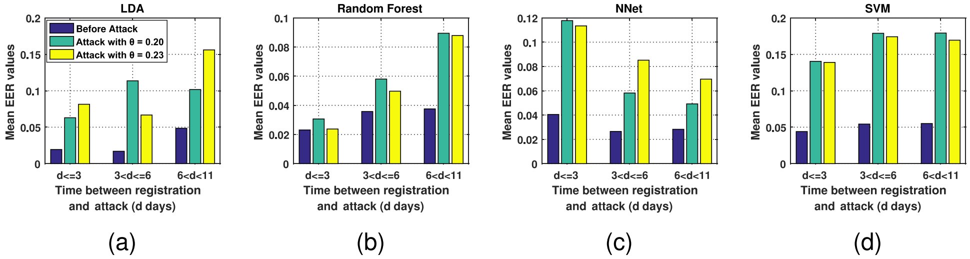


Fig. 8. Mean EER values before and after attack for LDA (a), RF (b), NNet (c), and SVM (d) classifier–based systems with time difference between user registration and attack. Attack performance is shown with varying thresholds of $\theta = 0.20$ (green) and $\theta = 0.23$ (yellow).

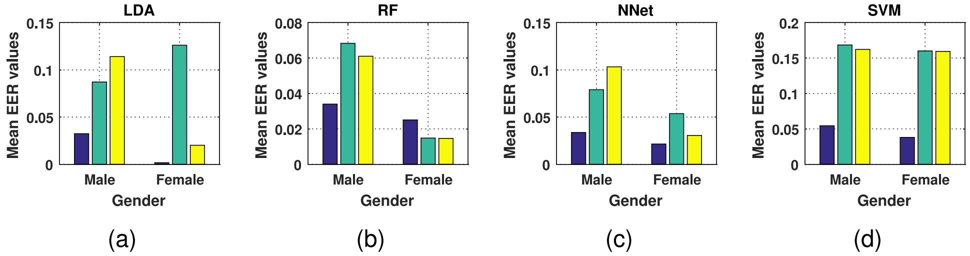


Fig. 9. Mean EER values before and after attack for LDA (a), RF (b), NNet (c), and SVM (d) classifier–based systems for male and female participants. Attack performance is shown with varying thresholds of $\theta = 0.20$ (green) and $\theta = 0.23$ (yellow). EER of the system before attack is shown with blue color.

*Attack performance for each user.* We repeated our attack for each user with varying values of $\theta$ as 0.20 and 0.23 (see Section 3). Figure 10 shows the attack performance on each user in our study for four different classification algorithms that were used to build the EEG-based authentication systems. It is observed from Figure 10 that there are significant increases in EER values with attack samples. This observation is valid for different $\theta$ values and for all classifiers. For each user, we observed an increase in mean EER values of the trained classifiers when tested with generated attack samples. Figure 10(e) shows the overall mean EER values computed for all users in our study.

*6.2.1 Attack Performance for Each User.* We generated $Fake_{EEG}$ signals for each user by leveraging their left hand motions features and then by leveraging their right hand motions features. To test the performance of our attack, we supplied generated $Fake_{EEG}$ feature vectors as the test sample to our Emotiv EEG-based authentication system. We repeated our attack for each user with varying values of $\theta$ as 0.20 and 0.23 (see Section 3).

*Attack Implemented Using Left Hand Motion Data.* Figure 10 shows the attack performance on each user in our study for four different classification algorithms that were used to build the EEG-based authentication systems. It is observed from Figure 10 that there are significant increases in EER values with attack samples. This observation is valid for different $\theta$ values and for all classifiers. For each user, we observed an increase in mean EER values of the trained classifiers when tested with generated attack samples. Figure 10(e) shows the overall mean EER values computed for all users in our study.

*Attack Implemented Using Right Hand Motion Data.* Figure 11 shows the attack performance on each user in our study for four different classification algorithms used to build the EEG-based authentication systems. Figure 11(e) shows the overall mean EER values computed for all users in our study. It is observed from Figure 11 that there are significant increases in EER values with attack samples. This observation is valid for different $\theta$ values and for all classifiers.

*6.2.2 Attack Performance with the Users' Gender.* We also analyzed the effects of the users' gender on the performance of the attack. Figure 12 shows the performance when the attack was implemented using left hand motion features, whereas Figure 13 is showing the performance of the attack implemented using the right hand motion features. Our results show that the attack was successful for both female and male subjects. The attack cases (green with $\theta = 0.20$ and yellow with $\theta = 0.23$) have higher mean EER values than the cases when the attack was not deployed (blue).

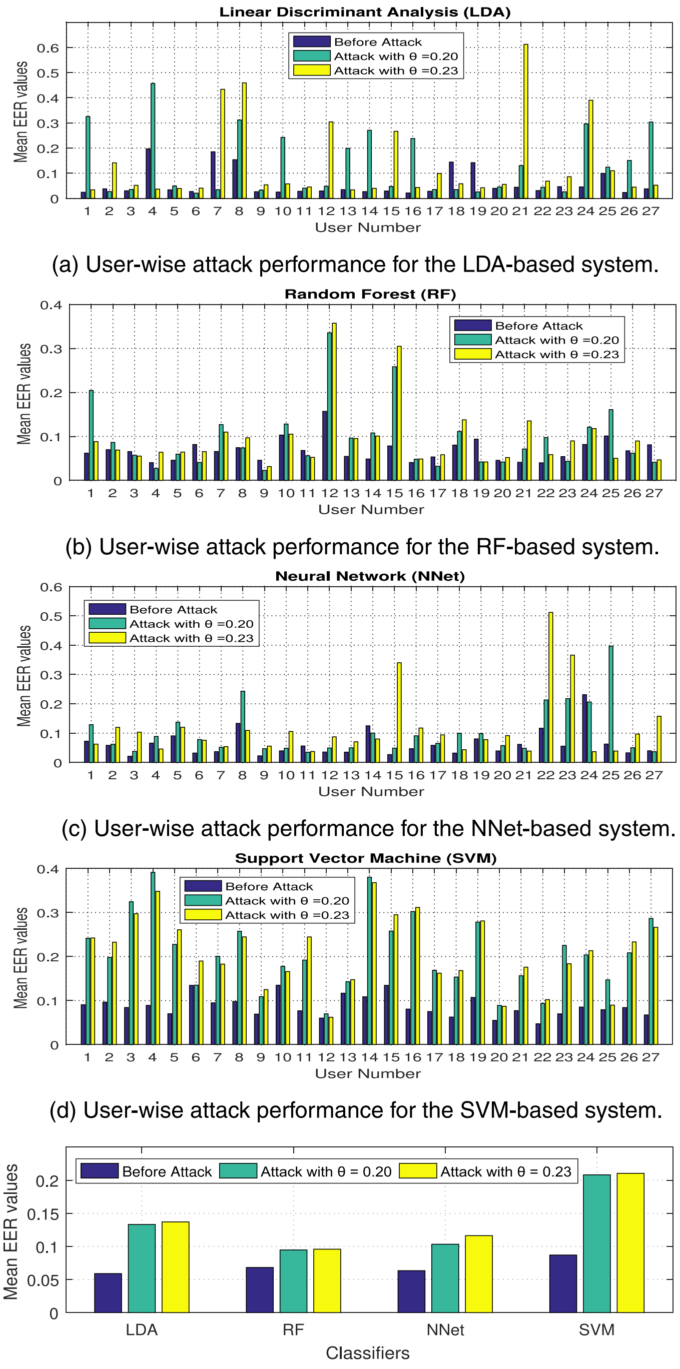
## 7 DISCUSSION

Our attack model requires the targeted user's hand movement patterns corresponding to the task performed for EEG-based authentication. The attack model utilizes the precomputed correlation between the hand movement signals and EEG signals for population data. The success of our attack model shows the need for a more robust test for EEG-based authentication systems against attacks such as ours. The work provides evidence that the popularly used zero-effort testing for EEG-based authentication system is not sufficient.

The limitations of our work are as follows:

(1) Our experiments use correlation from the training data of the users to develop a specific correlation of individual users who may have a part in the training data. The validity of correlations derived for populations not seen by the training data will present a more stringent test of the validity of our attack.

(2) Validity of the population correlation for individual attack needs to be examined in more detail. Our experiment verified the existence of a correlation between the EEG signal and the corresponding hand movement signal in two specific scenarios: (1) watching a video with emotional content and (2) typing about the video. Other scenarios such as password typing [3] and rest state [37] need to be analyzed.



(a) User-wise attack performance for the LDA-based system.

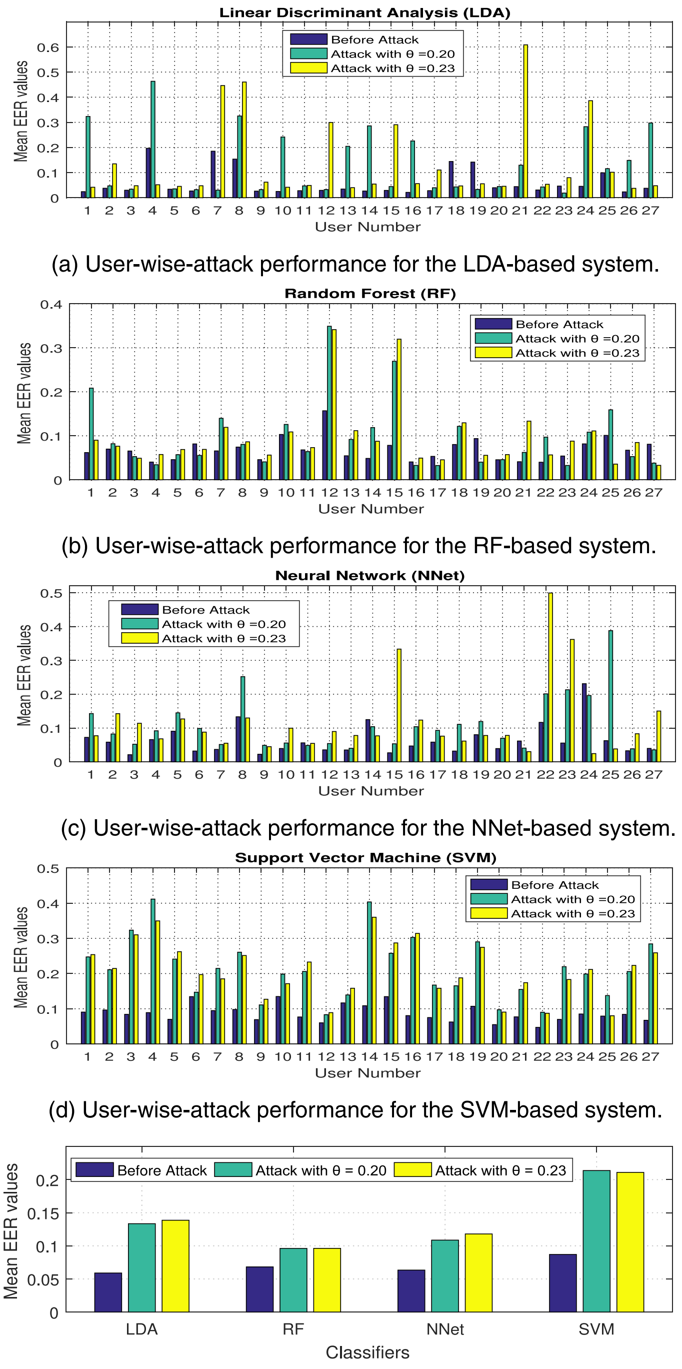
(b) User-wise attack performance for the RF-based system.

(c) User-wise attack performance for the NNet-based system.

(d) User-wise attack performance for the SVM-based system.

(e) Classifier-wise mean EER computed over all users.

Fig. 10. Attack performance on Emotiv-based EEG signals using left hand motion signals. Mean EER values before and after user-specific attack for LDA (a), RF (b), NNet (c), and SVM (d), and the mean EER before and after attack computed over all users (e). Attack performance is shown with varying thresholds of $\theta$= 0.20 (green) and $\theta$ = 0.23 (yellow).



(a) User-wise-attack performance for the LDA-based system.

(b) User-wise-attack performance for the RF-based system.

(c) User-wise-attack performance for the NNet-based system.

(d) User-wise-attack performance for the SVM-based system.

(e) Classifier-wise mean EER computed over all users.

Fig. 11. Attack performance on Emotiv-based EEG signals using right hand motion signals. Mean EER values before and after user-specific attack for LDA (a), RF (b), NNet (c), and SVM (d), and the mean EER before and after attack computed over all users (e). Attack performance is shown with varying thresholds of $\theta = 0.20$ (green) and $\theta = 0.23$ (yellow).

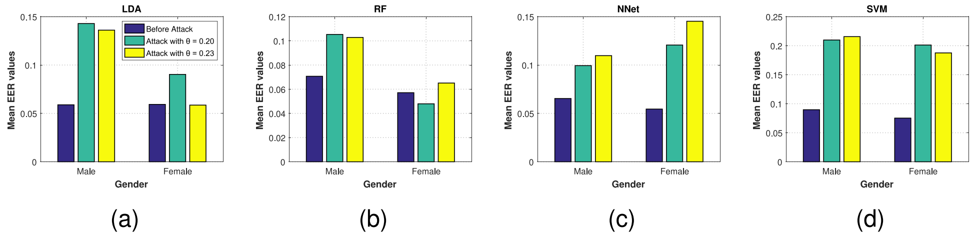


Fig. 12. Attack on Emotiv-based EEG using left hand motion data. Mean EER values before and after the attack for LDA (a), RF (b), NNet (c), and SVM (d) classifier-based systems for male and female participants. Attack performance is shown with varying thresholds of $\theta = 0.20$ (green) and $\theta = 0.23$ (yellow). EER of the system before the attack is shown with blue color.

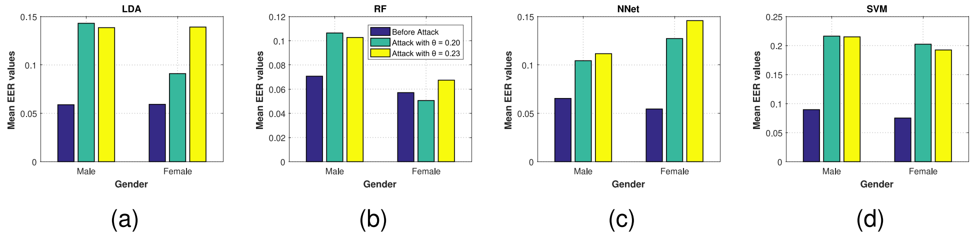


Fig. 13. Attack on Emotiv-based EEG using right hand motion data. Mean EER values before and after the attack for LDA (a), RF (b), NNet (c), and SVM (d) classifier–based systems for male and female participants. Attack performance is shown with varying thresholds of $\theta = 0.20$ (green) and $\theta = 0.23$ (yellow). EER of the system before the attack is shown with blue color.

(3) Other EEG-based authentication methods that use different verification approaches need to be analyzed for the existence of correlation and the effect of the correlation of EEG signals with other easily recordable signals.
(4) The article presents an analysis on a dataset collected from 59 volunteer participants, where 13 participants were female and the other 46 were male participants. Because the number of female participants is less than the number of male participants, the generalizability of results pertaining to female correlations needs to be validated. Since many studies show a significant difference in male and female brainwave signals [9, 50], there is a need for more detailed gender-specific study.
(5) In our data collection experiments, participants were briefed about the hypothesis of the study before the data collection session as per our IRB guidelines. This knowledge might have some influence and might have resulted in deviations from normal behavior of the volunteer participants.

## 8 CONCLUSION AND FUTURE WORK

In this study, we successfully demonstrated that hand movement patterns and brain activity patterns show a strong level of intrinsic correlation. We also showed the possibility of exploiting this correlation to build an attack on EEG-based authentication systems, exposing a previously invalidated security threat. Our work provides evidence that the widely used zero-effort testing is not sufficient for EEG-based authentication systems. Our findings call for more stringent performance evaluation of EEG-based authentication systems and motivate research into technologies to build a more effective defense against forgery attacks.

Our future work consists of building a sophisticated fusion methodology such that it improves the present EEG-based authentication mechanism and is less vulnerable to forgery attacks such as ours. We also plan to examine how the diverse emotional states of a human affect the attack model.

# APPENDIX

## A LIST OF VIDEOS USED IN OUR STUDY

We used a total of 40 selected videos from video networking websites in our experiments. The videos were categorized into two different categories; (1) videos with happy emotional content and (2) videos with sad emotional content. The videos with happy emotional content are expected to invoke happy emotion when watched, whereas videos with sad emotional content are believed to invoke sad emotion.

### Videos with Happy Emotional Content

(1) First Aid | Mr. Bean Official https://www.youtube.com/watch?v=P9ju80SMWZY
(2) Mr. Bean in Room 426 - Part 3/5 | Mr. Bean Official, url: https://www.youtube.com/watch?v=refziTk-giA
(3) Charlie Chaplin boxing, url: https://www.youtube.com/watch?v=wiKZAA-rFtg
(4) “Interview with An Applicant” - Sketch Comedy, url: https://www.youtube.com/watch?v=7W_qrc-TkR8
(5) Louis CK - Indians, White People and God’s Earth, url: https://www.youtube.com/watch?v=YWZkwuILn_s
(6) Is This Free? (Short Comedy Film), url: https://www.youtube.com/watch?v=sxCWB47ZCLQ
(7) Short film “The Elevator”, url: https://www.youtube.com/watch?v=Q-TQQE1y68c
(8) Louis CK - On divorce and on Social Media, url: https://www.youtube.com/watch?v=92kDUiN1zLQ
(9) Louis CK: On driving - Oh My God (HD), url: https://www.youtube.com/watch?v=x8062QEFk5g
(10) The Expert (Short Comedy Sketch), https://www.youtube.com/watch?v=BKorP55Aqvg
(11) Cute Baby Videos | Funny Vines 2018, url: https://www.youtube.com/watch?v=2aK8hy50fS4
(12) That’s One Way to Do It! August 2019 AFV, url: https://www.youtube.com/watch?v=lKol2GOSPeM
(13) The Expert: IT Support (Short Comedy Sketch), url: https://www.youtube.com/watch?v=ZOzzRlc_qho
(14) Tom and Jerry | Invisible Mouse + Halloween Party, url: https://www.youtube.com/watch?v=TF8My2RFl-U
(15) Tom & Jerry | You’re Still My Baby, Baby. url: https://www.youtube.com/watch?v=PZcHR_zMRgU
(16) Sound of Music- So Long, Farewell, url: https://www.youtube.com/watch?v=-nRU5RIDWXU
(17) This Is How I Talk – SNL, url: https://www.youtube.com/watch?v=f8PXvqYpGCM
(18) Tom & Jerry - Funny Moments, url: https://www.youtube.com/watch?v=H4PAKzzThUk
(19) DO-RE-MI, url: https://www.youtube.com/watch?v=dbsJ2DZoiQI
(20) FROZEN | Let It Go Sing-along | Official Disney UK, url: https://www.youtube.com/watch?v=L0MK7qz13bU
(21) The Big Bang Theory - Funniest Moments, url: https://www.youtube.com/watch?v=s5tFMfi47aE

### Videos with Sad Emotional Content

(1) Don’t text and drive - Graphic commercial, url: https://www.youtube.com/watch?v=wgyTBYjc0j8
(2) Ellie and Carl’s relationship through time, Sad scene, url: https://www.youtube.com/watch?v=F2bk_9T482g
(3) LIFE ISN’T PERFECT - Sad Story, url: https://www.youtube.com/watch?v=stdvLavp5Js
(4) “Uri” - by Adrian Chaves & Jose Alegria, url: https://www.youtube.com/watch?v=5p3fWbEZ8R4
(5) A sad story that will make you cry, url: https://www.youtube.com/watch?v=m4p9Xk95vsI
(6) HACHIKO- Try not to cry, url: https://www.youtube.com/watch?v=b54YYhHIHag
(7) Trois Petits Chats, url: https://www.youtube.com/watch?v=CZsIxEnN0k0
(8) “Father” a sad short film, url: https://www.youtube.com/watch?v=sXXbFpwkHrM
(9) ‘Falling in Love’ - Student Animated Short Film. url: https://www.youtube.com/watch?v=Zp85xOn71v8
(10) Sister A Sad Story (Cancer), url: https://www.youtube.com/watch?v=UwmrrCSFEPE
(11) DAD (Short Movie SAD STORY), url: https://www.youtube.com/watch?v=WNGibOESRQA

(12) Sad Movie Scenes HD part 5, url: https://www.youtube.com/watch?v=uHAkdltC0zw
(13) Sad Movie Scenes HD part 6, url: https://www.youtube.com/watch?v=pVWj8Jg3h6Y
(14) Sad Movie Scenes HD part 7, url: https://www.youtube.com/watch?v=bsxXkLRy5aU
(15) Sad Movie Scenes HD part 9, url: https://www.youtube.com/watch?v=MMne1I8Rqi4
(16) NF - Goodbye Lyric Video, url: https://www.youtube.com/watch?v=EDw_d2_HKcA
(17) Short Sad Story, url: https://www.youtube.com/watch?v=nyeh23XcGnA
(18) Another Sad Love Story, url: https://www.youtube.com/watch?v=RCNbm8l5nGw
(19) Titanic |1997| Sinking Scenes, url: https://www.youtube.com/watch?v=MPklvytosy4

## B DISCRETE WAVELET TRANSFORM

Wavelet transforms can be specified in terms of a low-pass filter $lp$, which satisfies the standard quadrature mirror condition. The complementary high-pass filter is $hp$. A sequence of filters with increasing length in time domain is expressed as

$$lp_{j+1}(q) = [lp]_{\uparrow 2^j} lp_j(q), \quad hp_{j+1}(q) = [hp]_{\uparrow 2^j} lp_j(q),$$

where the symbol $[.]_{\uparrow p}$ indicates the up-sampling by a factor of $p$, $q$ is the equally sampled discrete time, and $hp$ is the complementary high-pass filter.

The normalized wavelet and scale basis functions $\mathcal{W}_{j,m}(p)$ and $\mathcal{S}_{j,m}(p)$ are defined as

$$\mathcal{W}_{j,m}(p) = 2^{j/2} * lp_j(p - 2^i * m)$$

and

$$\mathcal{S}_{j,m}(p) = 2^{j/2} * hp_j(p - 2^i * m),$$

where $2^{j/2}$ is an inner product normalization, and $j$ and $m$ are the scale and translation parameters, respectively. The DWT decomposition is described as

$$l_{(j)}(m) = A(p) * \mathcal{W}_{j,m}(p)$$

and

$$h_{(j)}(m) = A(p) * \mathcal{S}_{j,m}(p),$$

where $l_{(j)}(m)$ and $h_{(j)}(m)$ are the approximation and detail coefficients at resolution $j$, respectively [2]. $A(p)$ is the $p$th sample of the NeuroSky signal $A$.

The multi-resolution decomposition technique of signal $A(p)$ is schematically shown in Figure 14. Each stage has two digital filters and two down samplers by 2.

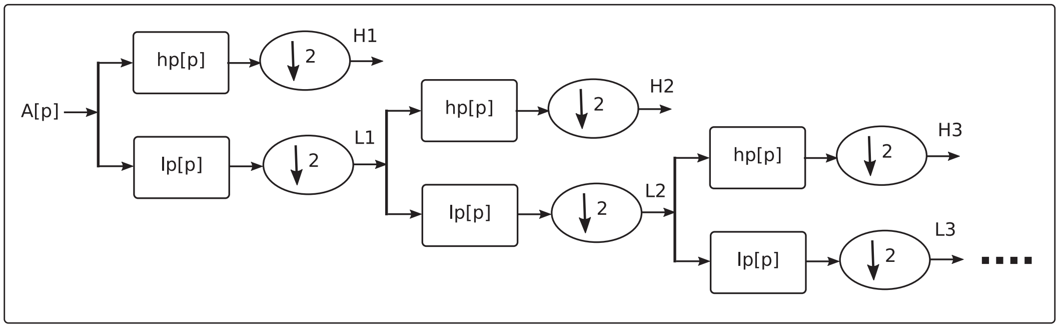


Fig. 14. Sub-band decomposition of DWT implementation. hp[p], high-pass filter; lp[p] low-pass filter.

## C STATISTICAL SIGNIFICANCE OF ERROR RATES—COMPARATIVE ANALYSIS OF THE ATTACK PERFORMANCE

The statistical procedure called *mixed effects analysis of variance* can be used to test the statistical significance of differences between mean error rates of the attack performance with original authentication performance. Mixed effects ANOVA test can be performed if the underlying distribution follows Gaussian behavior. We first used the Shapiro-Wilk statistical significance test under the null hypothesiswhen the mean EER differences were Gaussian for each of the classifiers used in our experiments. We rejected the null hypothesis at the 5% significance level for all tests except SVM($\theta = 2.0$) and SVM($\theta = 2.3$). Since the Shapiro-Wilk test failed to reject these two classifiers, we employed the K-S test for normality for all classifiers. The procedure resulted in a significance probability less than $10^{-7}$ for all tests. Hence, we rejected the null hypothesis for all the pairs.

Since the mean EER differences do not exhibit Gaussian behavior, we choose to use the Friedman method to test statistical significance in differences of mean EERs. The Friedman test resulted in a significance probability less than 0.04 for all pairs except LR($\theta = 2.0$) and LR($\theta = 2.3$) (Table 4). Therefore, we failed to reject the null hypothesis when methods were equally accurate on average for RF at the 4% of significance level. We rejected the null in other cases. We also employed the Wilcoxon test with the null hypothesis and drew the same conclusions as with the Friedman test (see Table 4).

Table 4. Results of the Statistical Test for Significance of Difference in the Mean EERs Obtained for Attack on Neurosky-Based EEG with Threshold $\theta = 2.0$ and $\theta = 2.3$ Using LR-, LDA-, NNet-, and SVM-Based Machine Learning Classifiers

| **Classifiers** | ***p*-Value** | | |
|---|---|---|---|
| | **Normality** | **Performance Test** | |
| | **KS Test** | **Friedman** | **Wilcoxon** |
| LR ( $\theta = 2.0$) | 4.47E-07 | 0.4795 | 0.085377 |
| LR ( $\theta = 2.3$) | 4.47E-07 | 0.4795 | 0.120659 |
| LDA ( $\theta = 2.0$) | 3.69E-06 | 0.004556 | 0.004615 |
| LDA ( $\theta = 2.3$) | 4.50E-06 | 0.00729 | 0.018675 |
| NNet ( $\theta = 2.0$) | 1.91E-07 | 0.000101 | 0.000109 |
| NNet ( $\theta = 2.3$) | 4.92E-07 | 0.033895 | 0.01847 |
| SVM ( $\theta = 2.0$) | 4.16E-07 | 7.43E-07 | 1.86E-06 |
| SVM ( $\theta = 2.3$) | 2.32E-07 | 1.14E-07 | 1.28E-06 |

## ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their detailed comments.

## REFERENCES

[1] NeuroSky. 2017. ThinkGear Serial Stream Guide. Retrieved September 1, 2019 from http://developer.neurosky.com/docs/doku.php?id=thinkgear_communications_protocol.

[2] M. Akay. 1997. Wavelet applications in medicine. *IEEE Spectrum* 34, 5 (May 1997), 50–56. DOI: https://doi.org/10.1109/6.590747

[3] R. Alomari, M. V. Martin, S. MacDonald, C. Bellman, R. Liscano, and A. Maraj. 2017. What your brain says about your password: Using brain-computer interfaces to predict password memorability. In *Proceedings of the 2017 15th Annual Conference on Privacy, Security, and Trust (PST'17)*. 127–12709. DOI: https://doi.org/10.1109/PST.2017.00024

[4] Corey Ashby, Amit Bhatia, Francesco Tenore, and Jacob Vogelstein. 2011. Low-cost electroencephalogram (EEG) based authentication. In *Proceedings of the 5th International IEEE/EMBS Conference on Neural Engineering (NER'11)*.442–445. DOI: https://doi.org/10.1109/NER.2011.5910581

[5] Tony Beltramelli and Sebastian Risi. 2015. Deep-spying: Spying using smartwatch and deep learning. arXiv:1512.05616.

[6] M. Bertram, T. Sattel, S. Hohmann, and J. Wiegert. 2008. Monte-Carlo scatter correction for cone-beam computed tomography with limited scan field-of-view.*Proceedings of SPIE 6913, Medical Imaging 2008: Physics of Medical Imaging* 6913 (2008), Y9131. DOI: https://doi.org/10.1117/12.771103

[7] Christopher M. Bishop. 2006. *Pattern Recognition and Machine Learning*. Information Science and Statistics, Vol. 4. Springer-Verlag, New York, NY. DOI: https://doi.org/10.1117/1.2819119 arXiv:0-387-31073-8

[8] Kamil Burda. 2016. Authenticating users based on how they pick up smartphones. In *Proceedings of the 12th Student Research Conference in Informatics and Information Technologies*. 8.

[9] Giulia Cartocci, Patrizia Cherubino, Dario Rossi, Enrica Modica, Anton Giulio Maglione, Gianluca Di Flumeri, and Fabio Babiloni. 2016. Gender and age related effects while watching TV advertisements: An EEG study. *Computational Intelligence and Neuroscience* 2016 (2016), 3795325.

[10] Alberto Compagno, Mauro Conti, Daniele Lain, and Gene Tsudik. 2017. Don't Skype & Type! Acoustic eavesdropping in Voice-over-IP. In *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIA CCS'17)*. ACM, New York, NY, 703–715.

[11] P. A. Devijver and J. Kittler. 1982. *Pattern Recognition: A Statistical Approach*. Prentice Hall, Englewood Cliffs, NJ.

[12] Alan Ferrari, Daniele Puccinelli, and Silvia Giordano. 2015. Gesture-based soft authentication. In *Proceedings of the IEEE 11th International Conference on Wireless and Mobile Computing, Networking, and Communications (WiMob'15)*. IEEE, Los Alamitos, CA, 771–777.

[13] Jonathan B. Freeman, Rick Dale, and Thomas A. Farmer. 2011. Hand in motion reveals mind in motion. *Frontiers in Psychology* 2 (Dec. 2011), 1–6.

[14] Rohit Goyal, Nicola Dragoni, and Angelo Spognardi. 2016. Mind the tracker you wear: A security analysis of wearable health trackers. In *Proceedings of the 31st Annual ACM Symposium on Applied Computing (SAC'16)*. ACM, New York, NY, 131–136.

[15] Qiong Gui, Wei Wang, Zhanpeng Jin, Mariz V. Ruiz-Blondet, and Sarah Laszlo. 2016. A residual feature-based replay attack detection approach for brainprint biometric systems. In *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS'16)*. IEEE, Los Alamitos, CA, 1–6.

[16] T. Inouye, K. Shinosaki, H. Sakamoto, S. Toi, S. Ukai, A. Iyama, Y. Katsuda, and M. Hirano. 1991. Quantification of EEG irregularity by use of the entropy of the power spectrum. *Electroencephalography and Clinical Neurophysiology* 79, 3 (1991), 204–210. DOI: https://doi.org/10.1016/0013-4694(91)90138-T

[17] A. H. Johnston and G. M. Weiss. 2015. Smartwatch-based biometric gait recognition. In *Proceedings of the 7th IEEE International Conference on Biometrics Theory, Applications, and Systems (BTAS'15)*. 1–6. DOI: https://doi.org/10.1109/BTAS.2015.7358794

[18] A. Kandaswamy, C. Sathish Kumar, Rm. Pl. Ramanathan, S. Jayaraman, and N. Malmurugan. 2004. Neural classification of lung sounds using wavelet coefficients. *Computers in Biology and Medicine* 34, 6 (2004), 523–537.

[19] J. F. Kenney and E. S. Keeping.1962. Correlation theory. *Mathematics of Statistics* (3rd ed.). Van Nostrand, Princeton, NJ, 252–285. https://babel.hathitrust.org/cgi/pt?id=mdp.39015078612788&view=2up&seq=6.

[20] W. Khalifa, A. Salem, M. Roushdy, and K. Revett. 2012. A survey of EEG based user authentication schemes. In *Proceedings of the 8th International Conference on Informatics and Systems (INFOS'12)*. IEEE, Los Alamitos, CA, 55–60.

[21] Juris Klonovs, Christoffer Kjeldgaard Petersen, Henning Olesen, and Allan Hammershoj. 2013. ID proof on the go: Development of a mobile EEG-based biometric authentication system. *IEEE Vehicular Technology Magazine* 8, 1 (2013), 81–89.

[22] Martin Kracheel, Walter Bronzi, and Hamed Kazemi. 2014. A wearable revolution: Is the smartwatch the next small big thing? *IT ONE Magazine* 7 (Dec. 2014), 18–19.

[23] Rajesh Kumar, Vir V. Phoha, and Rahul Raina. 2016. Authenticating users through their arm movement patterns. arXiv:1603.02211.

[24] Siaw-Hong Liew, Yun-Huoy Choo, Yin Fen Low, and Zeratul I. Mohd Yusoh. 2017. EEG-based biometric authentication modelling using incremental fuzzy-rough nearest neighbour technique. *IET Biometrics* 7, 2 (2017), 145–152.

[25] Feng Lin, Kun Woo Cho, Chen Song, Zhanpeng Jin, and Wenyao Xu. 2018. Exploring a secure and truly cancelable brain biometrics for smart headwear. In *Proceedings of the 16th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'18)*. IEEE, Los Alamitos, CA, 1–16.

[26] J. Liu and W. Sun. 2016. Smart attacks against intelligent wearables in people-centric Internet of Things. *IEEE Communications Magazine* 54, 12 (Dec. 2016), 44–49. DOI: https://doi.org/10.1109/MCOM.2016.1600553CM

[27] Jian Liu, Yan Wang, Gorkem Kar, Yingying Chen, Jie Yang, and Marco Gruteser. 2015. Snooping keystrokes with mm-level audio ranging on a single phone. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (MobiCom'15)*. ACM, New York, NY, 142–154.

[28] Chris Xiaoxuan Lu, Bowen Du, Hoongkai Wen, Sen Wang, Andrew Markham, Ivan Martinovic, Yiran Shen, and Niki Trigoni. 2017. Snoopy: Sniffing your smartwatch passwords via deep sequence learning. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 4 (Dec. 2017), 1–29.

[29] Duo Lu, Kai Xu, and Dijiang Huang. 2017. A data driven in-air-handwriting biometric authentication system. In *Proceedings of the 2017 IEEE International Joint Conference on Biometrics (IJCB'17)*. IEEE, Los Alamitos, CA, 531–537.

[30] Emanuele Maiorana and Patrizio Campisi. 2018. Longitudinal evaluation of EEG-based biometric recognition. *IEEE Transactions on Information Forensics and Security* 13, 5 (May 2018), 1123–1138.

[31] Anindya Maiti, Oscar Armbruster, Murtuza Jadliwala, and Jibo He. 2016. Smartwatch-based keystroke inference attacks and context-aware protection mechanisms. In *Proceedings of the 11th ACM Asia Conference on Computer and Communications Security (ASIA CCS'16)*. ACM, New York, NY, 795–806.

[32] Anindya Maiti, Murtuza Jadliwala, Jibo He, and Igor Bilogrevic. 2015. (Smart)watch your taps: Side-channel keystroke inference attacks using smartwatches. In *Proceedings of the ACM International Symposium on Wearable Computers (ISWC'15)*. ACM, New York, NY, 27–30.

[33] Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. 2011. (sp)iPhone: Decoding vibrations from nearby keyboards using mobile phone accelerometers. In *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11)*. ACM, New York, NY, 551–562.

[34] Ivan Martinovic, Doug Davies, Mario Frank, Daniele Perito, Tomas Ros, and Dawn Song. 2012. On the feasibility of side-channel attacks with brain-computer interfaces. In *Proceedings of the 21st USENIX Security Symposium (USENIX Security'12)*. 143–158.

[35] Rene Mayrhofer and Hans Gellersen. 2007. Shake well before use: Authentication based on accelerometer data. In *Proceedings of the International Conference on Pervasive Computing*. 144–161.

[36] Byoung-Kyong Min, Heung-II Suk, Min-Hee Ahn, Min-Ho Lee, and Seong-Whan Lee. 2017. Individual identification using cognitive electroencephalographic neurodynamics. *IEEE Transactions on Information Forensics and Security* 12, 9 (Sept. 2017), 2159–2167.

[37] T. Nakamura, V. Goverdovsky, and D. P. Mandic. 2018. In-ear EEG biometrics for feasible and readily collectable real-world person authentication. *IEEE Transactions on Information Forensics and Security* 13, 3 (March 2018), 648–661. DOI: https://doi.org/10.1109/TIFS.2017.2763124

[38] Xian Pan, Zhen Ling, Aniket Pingley, Wei Yu, Nan Zhang, and Xinwen Fu. 2012. How privacy leaks from Bluetooth mouse? In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS'12)*. ACM, New York, NY, 1013–1015.

[39] Tien Pham, Wanli Ma, Dat Tran, Phuoc Nguyen, and Dinh Phung. 2014. Multi-factor EEG-based user authentication. In *Proceedings of the International Joint Conference on Neural Networks (IJCNN'14)*. IEEE, Los Alamitos, CA, 4029–4034.

[40] Maria V. Ruiz-Blondet, Zhanpeng Jin, and Sarah Laszlo. 2016. CEREBRE: A novel method for very high accuracy event-related potential biometric identification. *IEEE Transactions on Information Forensics and Security* 11, 7 (July 2016), 1618–1629.

[41] Maria V. Ruiz-Blondet, Zhanpeng Jin, and Sarah Laszlo. 2017. Permanence of the CEREBRE brain biometric protocol. *Pattern Recognition Letters* 95, 1 (Aug. 2017), 37–43.

[42] Allen Sarkisyan, Ryan Debbiny, and Ani Nahapetian. 2015. WristSnoop: Smartphone PINs prediction using smartwatch motion sensors. In *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS'15)*. IEEE, Los Alamitos, CA, 1–6.

[43] Abdul Serwadda and Vir V. Phoha. 2013. Examining a large keystroke biometrics dataset for statistical-attack openings. *ACM Transactions on Information and System Security* 16, 2 (Sept. 2013), Article 8, 30 pages. DOI: https://doi.org/10.1145/2516960

[44] A. Serwadda, V. V. Phoha, S. Poudel, L. M. Hirshfield, D. Bandara, S. E. Bratt, and M. R. Costa. 2015. fNIRS: A new modality for brain activity-based biometric authentication. In *Proceedings of the 7th IEEE International Conference on Biometrics Theory, Applications, and Systems (BTAS'15)*. IEEE, Los Alamitos, CA, 1–7.

[45] D. Shukla, S. Chen, Y. Lu, P. P. Kundu, R. Malapati, S. Poudel, Z. Jin, and V. V. Phoha. 2019. Brain Signals and the Corresponding Hand Movement Signals Dataset (BS-HMS-Dataset). Retrieved April 19, from https://ieee-dataport.org/open-access/brain-signals-and-corresponding-hand-movement-signals-dataset-bs-hms-dataset.

[46] D. Shukla, G. Wei, D. Xue, Z. Jin, and V. V. Phoha. 2018. Body-taps: Authenticating your device through few simple taps. In *Proceedings of the 2018 IEEE 9th International Conference on Biometrics Theory, Applications, and Systems (BTAS'18)*. 1–8. DOI: https://doi.org/10.1109/BTAS.2018.8698602

[47] 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, 165–172.

[48] Abdulhamit Subasi. 2007. EEG signal classification using wavelet feature extraction and a mixture of expert model. *Expert Systems with Applications* 32, 4 (May 2007), 1084–1093.

[49] Kavitha P. Thomas and A. P. Vinod. 2017. Toward EEG-based biometric systems: The great potential of brain-wave-based biometrics. *IEEE Systems, Man, and Cybernetics Magazine* 3, 4 (Oct. 2017), 6–15.

[50] Michel J. A. M. Van Putten, Sebastian Olbrich, and Martijn Arns. 2018. Predicting sex from brain rhythms with deep learning. *Scientific Reports* 8, 1 (2018), 3069.

[51] Wouter van Vlaenderen, Jens Brulmans, Jo Vermeulen, and Johannes Schöning. 2015. WatchMe: A novel input method combining a smartwatch and bimanual interaction. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, New York, NY, 2091–2095.

[52] He Wang, Ted Tsung-Te Lai, and Romit Roy Choudhury. 2015. MoLe: Motion leaks through smartwatch sensors. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (MobiCom'15)*. ACM, New York, NY, 155–166.

[53] He Wang, Ted Tsung-Te Lai, and Romit Roy Choudhury. 2015. Mole: Motion leaks through smartwatch sensors. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, New York, NY, 155–166.

[54] Li Zhuang, Feng Zhou, and J. D. Tygar. 2005. Keyboard acoustic emanations revisited. In *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05)*. ACM, New York, NY, 373–382.

Received April 2019; revised October 2019; accepted November 2019