IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2023.0322000

De-authentication using Ambient Light Sensor

ANKIT GANGWAL[1], AASHISH PALIWAL[1], and , MAURO CONTI[2], (Fellow, IEEE)
[1]Centre for Security, Theory, and Algorithmic Research, International Institute of Information Technology Hyderabad, 500032, India
[2]Department of Mathematics, University of Padua, 35121, Italy

Corresponding author: Mauro Conti (e-mail: mauro.conti@unipd.it).

ABSTRACT While user authentication happens before initiating or resuming a login session, de-authentication detects the absence of a previously-authenticated user to revoke her currently active login session. The absence of proper de-authentication can lead to well-known *lunchtime* attacks, where a nearby adversary takes over a carelessly departed user's running login session. The existing solutions for automatic de-authentication have distinct practical limitations, e.g., extraordinary deployment requirements or high initial cost of external equipment.

In this paper, we propose ''DE-authentication using Ambient Light sensor'' (DEAL), a novel, inexpensive, fast, and user-friendly de-authentication approach. DEAL utilizes the built-in ambient light sensor of a modern computer to determine if the user is leaving her work-desk. DEAL, by design, is resilient to natural shifts in lighting conditions and can be configured to handle abrupt changes in ambient illumination (e.g., due to toggling of room lights). We collected data samples from 4800 sessions with 120 volunteers in 4 typical workplace settings and conducted a series of experiments to evaluate the quality of our proposed approach thoroughly. Our results show that DEAL can de-authenticate a departing user within 4 seconds with a hit rate of 89.15% and a fall-out of 7.35%. Finally, bypassing DEAL to launch a *lunchtime* attack is practically infeasible as it requires the attacker to either take the user's position within a few seconds or manipulate the sensor readings sophisticatedly in real-time.

INDEX TERMS Ambient light, De-authentication, Sensor, System security, Workplace.

I. INTRODUCTION

COMPUTER users in different establishments (e.g., universities, workplaces) often share workspace. These users either work on shared computers (e.g., in a library) or have a dedicated computer[1] (e.g., in an office). In either case, user authentication is critical to prevent any unauthorized access. Generally, the user authenticates via the secret PIN, password, or recently emerging biometrics-based techniques. However, such authentication typically happens only once while initiating the login session. After successful authentication, the user spends time to continuously use the computer and its services. If the user wants to leave her computer for whatever reason during this period, her currently active session must be locked/logged out; especially in shared workspace settings. Failure to do so can lead to *lunchtime* attacks [1], [2], where an adversary (typically an insider) gains access to the user's running session and engages in potentially undesirable activities.

To prevent such unauthorized access, either the user must terminate the running session by explicitly locking/logging out, or the system must automatically revoke the previously-authenticated session, i.e., de-authenticate the user. Oftentimes, the users are apathetic or lazy (especially when taking short breaks) and avoid terminating the session because logging in again can be annoying. On another side, de-authenticating the user frequently with too-short inactivity timeouts can aggravate the user while choosing a too-long inactivity timeout leaves room for *lunchtime* attacks [3].

Researchers from both academia and industry have put immense efforts into making the authentication techniques more robust, accurate, efficient, and convenient to use [4]. For instance, biometric-based authentication techniques impose less cognitive load on the users compared to the password-based approach. Nonetheless, password-based authentication still remains the most commonly used approach; mainly because it is intuitive and does not require any special hardware. But passwords have their demerits. First, recent technological advances are making passwords even more susceptible to cracking and potentially obsolete for use in the near future [5]. Second, passwords have no role in automatic user de-authentication, which means a separate mechanism is required. To this end, researchers have proposed different user de-authentication and continuous-authentication mech-

[1]We use the term 'computer' to equally represent a desktop and a laptop.

anisms. The state-of-the-art solutions (cf. Section II) require external equipments [1], [2], [6]–[11], are relatively expensive [1], [2], [9], [11], need physical customization or specific installation [1], [2], [7], [8], [12], are complex to deploy [2], [6], [7], involve regular maintenance [2], [8]–[10], or sometimes cause inconvenience to the user [6], [9]–[11]. Such limitations hinder a broader adoption of the existing solutions. Therefore, a solution is needed that can address all of these issues while handling the automatic user de-authentication process efficiently.

On the other side, consumer devices (e.g., phones, tablets, computers) are becoming sensor-rich to provide different useful functionalities. Ambient Light Sensor (ALS) is one such sensor. ALS has been pervasively found on phones and tablets. Nonetheless, ALS has recently started to become common on consumer-grade computers; primarily to comfort users' eyes by adapting the brightness and/or color tone of the screen in response to changing lighting conditions. ALS is generally mounted on a computer's display screen (e.g., as shown in FIGURE 1). A generic ALS is both fast and efficient in capturing changes in lighting conditions.

In this paper, we propose ''DE-authentication using Ambient Light sensor'' (DEAL), a novel de-authentication technique that utilizes the built-in ALS of a computer to decide whether the user is leaving her work-desk. In particular, DEAL takes advantage of the fact that a user normally sits/stands closer (suggested between 16 to 30 inches [13]) to the computer while working. Thus, the user can affect the illumination perceived by the computer's ALS when she moves away. In the simplest case, the user directly blocks the Line-of-Sight (LoS) path between ALS and the light source. Nonetheless, the ambient lighting conditions around the computer's ALS can also be influenced due to partial blocking of its LoS, shadowing it, or even reflection of light towards it from the departing user's body (cf. Section IV). We design DEAL to analyze the changes in lighting conditions via ALS readings to decide whether the user is departing from her work-desk. DEAL intrinsically addresses the above-mentioned issues of the state-of-the-art works by its design, i.e., **(1)** no external equipment is required as ALS is built-in a modern computer, **(2)** ALS is low-cost that too is already included in the computer's cost, **(3)** no physical installation of hardware is needed, **(4)** it is simple to deploy its software, **(5)** no periodic maintenance is required as an ALS is generally long-lasting and is powered directly by the computer, and **(6)** more importantly, it is user-friendly as the user is not required to carry or wear any apparatus.

Contribution: The contributions of our work are as follows:

1) We propose DEAL, a novel, unobtrusive, fast, and inexpensive de-authentication approach that is primarily designed for modern computers equipped with a built-in ALS. For backward compatibility (i.e., in the absence of a built-in ALS), existing computers may attach a USB-powered ALS to employ DEAL for de-authentication.
2) We thoroughly evaluate the performance of our proposed approach using data samples collected from 4800 sessions with 120 volunteers in 4 typical workplace settings. DEAL can attain an overall hit rate of 89.15% and a fall-out of 7.35% to de-authenticate the user within 4 seconds.
3) Finally, we compare DEAL with the state-of-the-art de-authentication approaches and delineate their respective advantages and limitations. We argue that the said performance of DEAL comes without any extraordinary requirements, customization, or expensive equipment, which makes it suitable for practical adoption.

Organization: The remainder of this paper is organized as follows. Section II presents a comparative summary of the related works. We elucidate our system and adversary models in Section III. We explain our proposed approach in Section IV and present its evaluation in Section V. Section VI elaborates on the salient features and potential limitations of our work. Finally, Section VII concludes the paper.

II. RELATED WORKS

Researchers from both academia and industry have put extensive efforts over the decades to develop effective user authentication techniques. To verify a user's identity, a typical authentication procedure utilize: (1) user's knowledge (e.g., password, pin) [5], (2) user's possession (e.g., token, keycard) [14], (3) user's physical attributes (e.g., biometrics) [15], (4) user's behavior (e.g., gestures, typing patterns, eye movements) [16], or (5) a combination of these to enable two-factor authentication [17], [18].

On another side, the need of user de-authentication arises after successful authentication of a user by the system. It is worth mentioning that a user's de-authentication by the system is independent of the authentication step. Therefore, the procedures for user de-authentication are distinct. One of the commonly used mechanisms for user de-authentication is the inactivity time-out approach. However, such an approach is ineffective because: (1) determining the optimal length of a static timeout interval is not straightforward, and (2) checking the user's presence/absence in front of the system is beyond its scope [3]. Given the significance of user de-authentication to prevent *lunchtime* attacks, different mechanisms have been proposed that aim at continuously establishing the user's presence/absence near the system.

Kaczmarek et al. [2] propose *Assentication* to profile user's sitting posture. In particular, *Assentication* installs 16 pressure sensors in an office chair to capture a hybrid biometric trait by combining user's behavioral and physiological characteristics. Though *Assentication* has low false positive and false negative rates, it has two key limitations. Firstly, it has low permanence, i.e., the hybrid biometric trait that it captures naturally changes over time for a given user. Secondly, the cost involved is not trivial, i.e., about $150 per chair. While eye movement tracking has been previously employed to authenticate users [16], Eberz et al. [1] use gaze tracking to prevent *lunchtime* attacks. Their system continuously tracks the user's eye movements with high accuracy. Since gaze tracking requires its user to keep their sight in a particular di-

rection, any head moment taking the sight away can generate false positives. Moreover, the cost of eye-tracking equipment hinders its large-scale adoption. Rasmussen et al. [6] propose a new biometric based on the human body's response to an electric pulse signal. Their approach involves applying a low-voltage pulse signal to user's one palm and measuring the body's response in the user's other palm. Apart from the cost of specialized hardware, engaging both hands of the users with pulse-response hardware restricts its general acceptability. Similarly, authors in the work [11] use ECGs to build continuous authentication systems that require end users to wear specialized hardware.

FADEWICH [7] measures the attenuation of wireless signals due to the human body for estimating the location of a user in a room, and the user is de-authenticated based on the user's estimated position. Their system uses 9 sensors in a fixed office setup to achieve very high accuracy. The major drawback of their approach is that the structure and setup of the office heavily affect the placement of sensors. Thus, each office requires customized positioning of sensors. Moreover, the presence and movements of other persons induce false positives. Keystroke dynamics technique [19] profiles a user's typing style. It is a simpler mechanism for continuous authentication, which is easily deployable and does not need specialized hardware. However, researchers [20] have shown that a brief training is sufficient to imitate typing pattern of the target users, even when their typing patterns are only partially known. DEB [8] instruments an office chair with two Bluetooth low-energy beacons. An application running on the target system monitors the signal strength of the received Bluetooth beacons. A human body present in the line of sight of a beacon affects the strength of the received signal, which is interpreted to keep the user logged into the system. Apart from interference due to nearby beacons, the lifespan and appropriate installation of Bluetooth beacons are the key concerns here. BLUFADE [12] employs deep learning algorithms to continuously detect the user's face in a webcam feed. However, using a camera feed for de-authentication carries apparent privacy concerns [21]. Thus, the authors propose to obfuscate the webcam with a physical blurring layer (e.g., anti-reflective obfuscating film) and use blurred images for face detection. Such an approach hampers the normal usage of the webcam. More importantly, it does not address the possibility of reconstructing the user's facial traits from blurry images.

ZIA [10] proposes monitoring the proximity of the user via a physical token borne by the user. Such a token periodically exchange information with the target system over a secure channel, and in the absence of such communication the user is de-authenticated by the system. Similarly, ZEBRA [9] uses a wrist bracelet fitted with a gyroscope, an accelerometer, and a radio. When the user interacts with the system, the bracelet captures and shares the wrist movements with an application running on the system. The application correlates the wrist movements with strokes on the keyboard to establish the user's presence. The key limitation of these approaches is that the user is required to always bear the token/bracelet. Furthermore, the tokens/bracelets also require periodic recharging or replacement of batteries. Relevant to our work, researchers have used ALS for user authentication [22] and tracking a user's activities [23]–[26].

III. SYSTEM AND ADVERSARY MODELS

In this section, we describe the system and adversary models we consider in our work. Section III-A presents the deployment scenario of the proposed de-authentication mechanism, and Section III-B elucidates the potential threat maneuvers of an adversary.

A. SYSTEM MODEL

DEAL is designed primarily for computers that come with a built-in ALS. The ALS data feed is processed in real-time by a simple application running in the background on the target computer. *Since the primary goal of any de-authentication mechanism is to prevent lunchtime attacks that are prevalent at typical workplaces [1], [2], [8], our proposed system is expected to be used in conventional workplace setups.* DEAL is absolutely unobtrusive. The user arrives at her work-desk, settles in her chair, logs into her computer via a preset authentication mechanism, uses the computer, and finally gets up to leave her desk. While the user prepares to depart from her desk, the system should automatically lock her out to prevent any unauthorized access. DEAL uses the light-intensity data feed from ALS to de-authenticate a departing user in real-time.

Contrary to state-of-the-art de-/continuous-authentication mechanisms [1], [6], [9], [19], DEAL does not need the user to interact continuously with the system. In fact, there can be situations when the user is present at the work-desk, but not interacting with the system. For instance, the user may be using a smartphone, reading a document, or simply watching a photo on the system. In such scenarios, de-authenticating the user due to her inactivity is undesirable and can be annoying.

B. ADVERSARY MODEL

We assume that the adversary has physical access to the user's office and, consequently, to her computer. An office colleague, a visitor in the office, or a housekeeping person are some representative examples of such an adversary that may be interested in getting access to her computer. Since the adversary does not know the login credentials required for logging in to the user's computer, the adversary's goal is to gain access to the user's running/authenticated session.

An adversary can try the following to bypass DEAL: (1) take the user's position (and control the computer) before DEAL can de-authenticate the user, or (2) manipulate light intensity perceived by her computer's ALS in such a way that DEAL does not de-authenticate the departing user at all. The former approach represents the typical *lunchtime* attack strategy. It is straightforward, yet effective if DEAL takes too long to de-authenticate. So, DEAL should operate fast enough to render such an attempt ineffective. The latter may involve

using sophisticated tools. For instance, the adversary may use a custom beam of light to compensate for the ALS readings affected due to the departing user. Such a maneuver requires the adversary to know the exact light intensity levels observed by the target ALS when the user is departing, which may be possible by: (1) installing an ALS near the target's ALS (ineffective; as it will visible to the user), (2) compromising the target machine to get such information (beyond the scope of the *lunchtime* attack), or (3) physically approaching the desk to measure/compensate readings (essentially the same as the first approach; a fast operating DEAL will handle it).

On another side, a different type of adversary can focus on triggering false de-authentications, e.g., by turning the lights on or off in the room. Although such an action can annoy the user by incorrectly de-authenticating her, the adversary does not get access to the user's computer. Nonetheless, toggling room lights is a part of routine office activities. Such sudden changes in lighting conditions significantly affect the ALS readings and induce large outliers. Therefore, we can easily identify and adapt to new lighting conditions if such large outliers in the ALS readings are consistently present.

IV. PROPOSED METHOD

We now present the conceptual and intrinsic details of DEAL. The fundamental task of a meaningful de-authentication technique is to determine the user's presence in front of the computer. To this end, DEAL utilizes data feed from the computer's ALS. The illumination perceived by ALS can be affected due to the user's movements. As a representative example, FIGURE 1 demonstrates that a user's movement of getting up/down from her chair can directly affect the ambient lighting conditions around the computer's ALS. Naturally, the scale and duration of such an impact depends on a variety of factors, e.g., how much/for how long the user has intersected the LoS path between ALS and the light source. We would like to highlight that though the light sources are typically roof-mounted (or, mounted high on the wall) in workplaces, the light source may not be in the direct LoS of ALS (cf. FIGURE 1). However, a user's movements can still affect the lighting conditions around ALS. In particular, due to partial[2] blocking, shadowing, or even reflection of light from the departing user's body. By measuring the changes in ambient lighting conditions through ALS readings, DEAL determines whether the user is departing from her work-desk, and subsequently de-authenticates her when required.

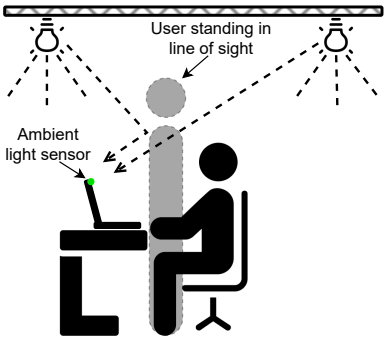


FIGURE 1. A representative depiction of affecting illumination perceived by ALS.

We make the following two reasonable assumptions in the implementation of DEAL: (1) the user will continue to work in the same position (standing or sitting) as she was in while initializing the current login session, and (2) if the user was sitting, she will get up before leaving. It is worth mentioning that if the user is standing while working at her work-desk, she will likely be blocking ALS' LoS. Such a case is simpler to handle for DEAL. For the sake of brevity, the rest of the paper proceeds with the scenario in which the user is sitting while using her computer.

The data feed from ALS can be modeled as a univariate time series of the observed light intensity. Thus, DEAL adopts an amended sliding window average-based approach for monitoring changes in lighting conditions. In particular, each reading (R, in lux) from ALS is compared against the average (μ) of running *window* as described in Eq. 1:

$$|\mu(window) - R| > \mu(window) * \Delta/100, \qquad (1)$$

where Δ (a natural number) is a predefined threshold. Such sliding window average-based methods are typically designed to identify an outlier outside of the current trend in a time series. However, a single outlier may not be sufficient in our case to distinguish the user's movements correctly. Because an ALS can provide several readings - according to its operating frequency (f, in Hz) - within a fraction of time. Moreover, different user activities can last for a different amount of time, e.g., the act of getting up and moving away from the computer can take up to a few seconds. So, it is intuitive to say that if a user's movement intercepts ALS's LoS for a longer period of time, then it will affect more ALS readings. We design DEAL to incorporate the duration of impact on ALS to distinguish user movements. To this end, we define a parameter η (in seconds). While Δ defines the minimum distance between an outlier and the average of running *window* (cf. Eq. 1), η specifies the minimum duration of time during which each consecutive[3] R should be an outlier

[2]In full blocking, the user totally obstructs the illumination received by ALS. The simplest example would be to cover ALS by hands. In partial blocking, the user partially hinders the light coming from a source. For instance, when a user intercepts ALS's LoS partially. The shadow of the user may or may not be falling around ALS in partial blocking. We call the former scenario shadowing, and the reflection of light is a natural phenomenon.

[3]Our current implementation requires each consecutive R in η duration of time to be an outlier. We are aware that such a design decision can result in false negatives even when one of the values is not an outlier. However, such a stricter control helps us evaluate the minimum performance of our system. We can certainly optimize such checks to improve the system. Currently, η works with a parameter ℓ to provide some relaxation to the system.

for recognizing the user to be departing and subsequently de-authenticating her.

Our system has two more parameters, i.e., ω (in seconds) and ℓ (in seconds). ω defines the size of the sliding window. ℓ is a tuning parameter that defines the maximum duration of time from the occurrence of the first outlier in a wave of outliers, during which the required consecutive outliers should occur for user de-authentication. From the virtues of their respective definitions, $\eta \leq \ell$. The system will not work if $\eta > \ell$, because it is impossible to have η (say 5 seconds) of consecutive outliers within a shorter ℓ (say 2 seconds). To simplify, ℓ separates waves of outliers. A larger value of ℓ enables us to process more values of R to satisfy constraints on η. However, a larger ℓ will cause a delay in resetting and recovering from a (short) wave of outliers. On another side, a larger value of η prevents false alarms due to subtle user movements. Algorithm 1 exhibits the pseudocode for the core logic of DEAL; that is re-initiated upon each successful login.

Algorithm 1 A simplified pseudocode for DEAL's core logic.

Input: $\Delta, \omega, \eta, \ell$

1: f := *FreqALS()* ▷ Sample ALS's operting frequency
2: ω' := $int(\omega * f)$ ▷ Align ω to ALS via f
3: η' := $int(\eta * f)$ ▷ Align η to ALS via f
4: *window* := List with recent ω' ALS readings
5: $temp_1 := 0$ ▷ Tracks number of consecutive outliers
6: $temp_2 := 0$ ▷ Stores time of first outlier in current wave
7: **while** *true* **do**
8: R := *readALS()*
9: **if** *(abs(*μ*(window)-R)* > μ*(window)**Δ/100) **then**
10: $temp_1 := temp_1 + 1$
11: **if** $temp_2 = 0$ **then**
12: $temp_2 := getTime()$
13: **end if**
14: **else**
15: $temp_1 := 0$
16: *window.append(R)* ▷ Append R to *window*
17: *window.pop(0)* ▷ Pop tail from *window*
18: **end if**
19: **if** $(temp_1 \geq \eta'$ && $(getTime() - temp_2) \leq \ell)$ **then**
20: *De-authenticate()*
21: **end if**
22: **if** $(temp_2 \neq 0$ && $(getTime() - temp_2) > \ell)$ **then**
23: *reSet(window, temp*$_1$*, temp*$_2$*)* ▷ Go to line 4
24: **end if**
25: **end while**

Since each ALS can operate at a different f, we begin with aligning ω and η to a given ALS via its f (lines 1-3). We next initialize the *window* and temporary variables (lines 4-6). We compare each reading from ALS with the mean of *window* (lines 7-9). If an outlier is found, a counter is incremented (line 10) while the time is recorded for the first outlier (lines 11-12). If R is not an outlier, the counter for outliers is reset (line 15), and R is adjusted in *window* (lines 16-17).

It is noteworthy that the running *window* average directly handles the natural shifts in lighting conditions. The user is de-authenticated if the required number of outliers (η') are found within ℓ seconds (lines 19-20). If the time elapsed since the first outlier in the current wave was seen exceeds ℓ, we reset *window* and temporary variables (lines 22-23).

V. EVALUATION

We describe our evaluation setup in Section V-A and data collection method in Section V-B. We discuss our experimental results in Section V-C.

A. EVALUATION SETUP

We evaluate DEAL in a typical office setup. To this end, we created an office space illuminated with both natural and artificial lights. As shown in FIGURE 2, our office setup has two ceiling-mounted white light sources that we keep on and a standard transparent window that allows natural light to come in. Though the half-glass door was kept closed during the experiments, its transparent glass portion in the upper half remained unobstructed.

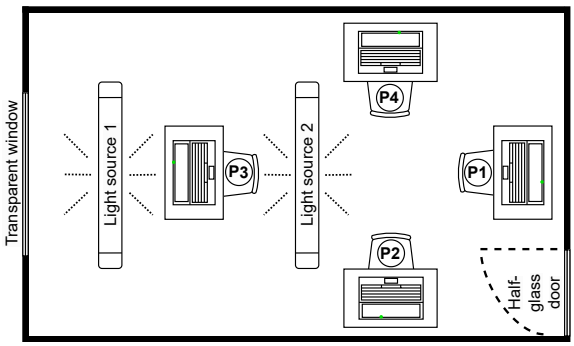


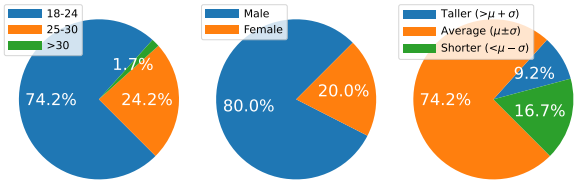
FIGURE 2. **The top view of our office setup.**

To emulate typical work-desk positions with respect to the lighting conditions, we set up four work-desks at different locations in the room (cf. FIGURE 2). In particular, position *P1* emulates a position with lower lighting since it is far from the light sources. Moreover, a user working in position *P1* may further block the illumination perceived by the computer's ALS. Being closer to light source 2, positions *P2* and *P4* represent normally illuminated positions. Lastly, position *P3* has copious lighting. In our experiments, we used a Lenovo ThinkPad Yoga 370 laptop. It comes with a built-in ALS. We modified *iio-sensor-proxy* [27] to capture readings from ALS. It is important to highlight that we periodically checked the health of our computer's ALS using an external phone-based ALS to avoid any bias or error in our ALS readings.

B. DATA COLLECTION

To collect ALS data for our experiments, we invited student volunteers to participate in our study. A total of 120 students volunteered for our study over a period of 90 days. Since the volunteers belong the student body of a large university, the

majority of them were naturally in the 18-24 age group. FIGURE 3 shows the distribution of the self-declared age groups, sex categories, and height classes[4] of the volunteers. It is noteworthy that our data collection activities were performed throughout different hours of the day.



(a) Age groups. (b) Sex categories. (c) Height classes.

FIGURE 3. The distribution of age, sex, and height of the volunteers.

Before beginning each instance of our data collection activity, we asked the volunteer to settle in a comfortable sitting/-working posture at a designated desk. After which we started recording the data from the computer's ALS. At the same time, we asked the volunteer to use the computer normally for about a minute. Next, the volunteer was asked to get up and move away from the chair. It is important to highlight that to prevent any interference due to our operational activities, we remotely operated our computer to capture the data from its ALS. We also documented the time when the volunteer was instructed to get up in the activity; mainly for post-processing and analysis. Each volunteer repeated the entire activity ten times each on the four work-desk positions (i.e., *P1*, *P2*, *P3*, and *P4*). Therefore, our dataset contains a total of 4800 data samples, i.e., 1200 data samples for each position. FIGURE 4 depicts a random set of data samples collected from different positions during our data collection activity. As discussed in Section V-A, the four work-desks experience different lighting conditions. This phenomenon is also evident from the light intensity scales shown in FIGURE 4 (a)-(d). We now briefly describe each plot shown in FIGURE 4.

As depicted in FIGURE 4(a), the ALS readings remain nearly constant as long as the user remains seated in *P1*. It is so because the body of the user is blocking the illumination coming from the distant light sources. The illumination perceived by ALS further drops when the user gets up. Intuitively, ALS receives a much higher illumination when the user completely moves away from the computer.

In case of *P2* and *P4*, the light sources are located on the right side and left side of the computer, respectively. ALS on our computer is located towards top-right of the screen. Thus, the chances of a sitting user shadowing LoS between ALS and the light sources are lesser in *P2* when compared with *P4*. As illustrated in FIGURE 4(b) and FIGURE 4(d), both *P2* and *P4* observe similar levels of light intensity. However, ALS readings in *P2* before and after the user moves away are at the same level, which implies that in this particular case, the user was not shadowing ALS. On another side, ALS readings in *P4* after the user moves away achieve similar levels as in the case of *P2*, which implies that in this particular case, the user was marginally shadowing ALS.

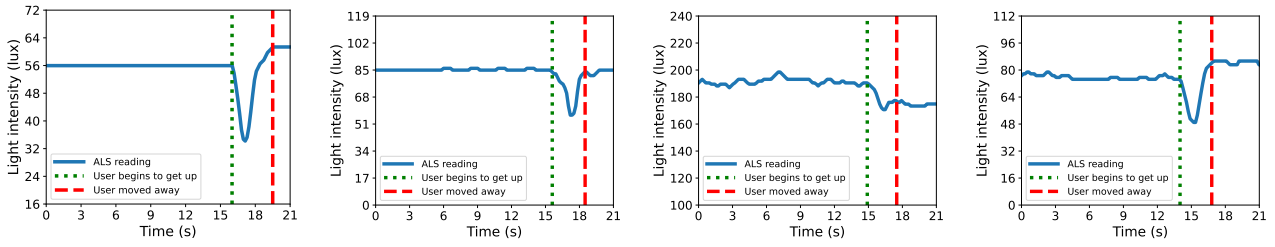
Unsurprisingly, the light intensity levels are the highest in *P3*. When the user moves away from *P3* in the particular case shown in FIGURE 4(c), ALS readings drop even lower than the levels when the user was sitting. A possible explanation of such a case is that the light coming from the sources in front of the user was being reflected by the user towards ALS when the user was sitting. Nevertheless, the ALS readings still clearly capture the movements of the departing user.

C. EXPERIMENTAL RESULTS

We empirically assess the quality of our proposed approach with real-world data. As explained in Section V-B, our dataset contains a total of 4800 data samples (i.e., 1200 data samples for each position) collected from 120 volunteers. We designed a series of experiments for a thorough analysis. We begin with investigating the general performance of DEAL. Here, we vary its input parameters to find a set of suitable configurations. Next, we study the effect of different positions (i.e., lighting conditions) considered in our work. Finally, we examine the impact of users' height. For a de-authentication system, false negatives are more severe than false positives. At the same time, true positives are also critical. Therefore, we report the hit rate[5] for each of our experiments.

[4]The volunteers declared their height classes based on the distribution of adult human heights [28].

[5]$Recall = Hit_{Rate} = \frac{TP}{TP+FN} = 1 - Miss_{Rate}$



(a) From *P1*. (b) From *P2*. (c) From *P3*. (d) From *P4*.

FIGURE 4. A random set of ALS data samples collected from different positions. It is worth reiterating that DEAL is re-initiated upon each successful login. Thus, the lighting conditions at the login time become the baseline (cf. line 4 in Algorithm 1) for DEAL, which then updates according to Algorithm 1.

An analysis of our data samples indicates that the volunteers took roughly two to four seconds to get up and move away from a work-desk. Thus, we set ℓ between 2 and 4 seconds to approximately cover the entire user movement. We observe that a portion of the ALS readings affected due to a user's movement can be treated, depending on the value of Δ, as non-outlier. It is especially witnessed for the values corresponding to the start and end of the movement; such values can still be within the threshold because the *window* is not updated during a wave of consecutive outliers (cf. lines 9, 14-17 in Algorithm 1). Therefore, we choose η between 1 and 2 seconds, which is about half the time the volunteers took to move. The value of ω is fixed at 3 seconds while Δ is chosen between 5 and 20 based on preliminary experiments.

We now discuss the generic performance of DEAL. TABLE 1 shows the hit rate of our system over the entire dataset of 4800 samples for different values of η, ℓ, and Δ. An increasing value of Δ corresponds to the fact that a user should affect ALS readings substantially for the system to recognize it as an outlier. Thus, DEAL becomes resistive with increasing values of Δ. Such behavior is evident in each row[6] of TABLE 1. The performance of our systems is affected by η in a similar way. A larger value of η requires a longer duration of outliers, which becomes even more challenging to attain under our stringent requirement of outliers' consecutiveness. A comparison of values[7] corresponding to increasing η over fixed ℓ and Δ reflects the same. On another side, a larger value of ℓ enables us to process more values of R. The performance of DEAL improves with increasing value[8] of ℓ over a given pair of η and Δ. From these experiments, we find $\Delta = 5$ and $\ell = 4s$ are suitable parameter values for DEAL. Since a larger η helps us avoid subtle user movements, we prefer $\eta = 1.5s$ over $\eta = 1.0s$ for our chosen values of Δ and ℓ. With these values of of Δ, ℓ, η, we observed a fall-out[9] of only 7.35%.

TABLE 1. Hit rate (%) for different values of η, ℓ, Δ.

η (s)	ℓ (s)	$\Delta = 5$	$\Delta = 10$	$\Delta = 15$	$\Delta = 20$
1.0	2	60.42	59.98	48.52	38.69
	3	71.92	70.13	63.54	51.83
	4	89.77	83.67	69.23	56.50
1.5	2	50.75	43.79	32.17	23.69
	3	71.77	66.67	52.35	40.60
	4	89.15	74.63	58.42	45.79
2.0	2	35.10	24.40	15.90	10.77
	3	66.27	53.21	37.44	27.10
	4	86.17	64.04	45.40	33.65

To understand the effect of different lighting conditions, we organize our dataset according to different positions (i.e., 1200 samples per position) considered in our study. TABLE 2 shows the hit rate of our system over different positions for $\eta = 1.5s$, $\ell = 4s$. Our results indicate that DEAL performs better in *P1*, where most volunteers blocked the illumination observed by ALS while working at the computer. We see the steepest decline in the hit rate at *P3*. Since *P3* has copious lighting, affecting ALS readings substantially for higher values of Δ is complex. *P2* and *P4*, which represent normally illuminated positions and have similar light intensity levels, obtain comparable results. Overall, our system performs competently for $\Delta = 5$ across different positions.

TABLE 2. Hit rate (%) over different positions for $\eta = 1.5s$, $\ell = 4s$.

Position	$\Delta = 5$	$\Delta = 10$	$\Delta = 15$	$\Delta = 20$
P1	91.75	82.50	67.67	56.75
P2	87.00	72.08	56.08	44.75
P3	90.08	70.83	53.33	35.42
P4	87.75	73.08	56.58	46.25

Next, we consider the users' height in our study. Due to a disparity in the number of volunteers per height class, we take 250 (roughly half of the taller class samples) randomly chosen samples from each height class. FIGURE 5 depicts the hit rate of DEAL over different height classes for $\eta = 1.5s$, $\ell = 4s$. While our results for $\Delta = 5$ are alike across different height classes, DEAL favors taller users for increasing values of Δ. The rationale for such behavior is related to the fact that a taller user likely remains in the LoS path of ALS while working, and when such a user moves away, the ALS readings are affected sufficiently for DEAL to operate properly.

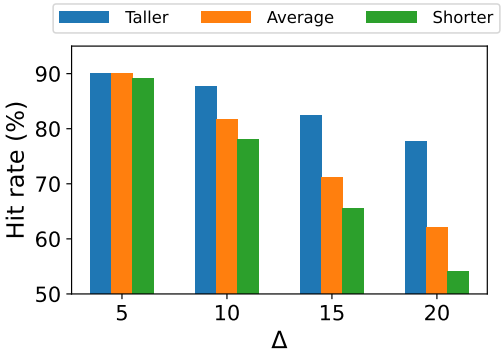


FIGURE 5. Hit rate (%) over different height classes for $\eta = 1.5s$, $\ell = 4s$.

To conclude, we argue that DEAL yields an overall effective performance. In particular, our system attains such scores without any extraordinary requirements or customization, as seen in the case of state-of-the-art solutions (cf. Section I). DEAL can de-authenticate the user within two to (more realistic) four seconds (i.e., based on the value of ℓ). In a real-world deployment, an enrollment step at the end user's work-desk can help tune the system to function even better.

VI. DISCUSSION

We specify the key attributes of our work in this section. Section VI-A compares DEAL with state-of-the-art user de-authentication schemes and highlights its salient features. Section VI-B discusses the potential limitations of DEAL.

[6] E.g., $60.42 > 59.98 > 48.52 > 38.69$; $\eta = 1s, \ell = 2s$.
[7] E.g., $60.42 > 50.75 > 35.10$; $\ell = 2s, \Delta = 5$.
[8] E.g., $60.42 < 71.92 < 89.77$; $\eta = 1s, \Delta = 5$.
[9] $Fall_{Out} = FalsePositive_{Rate} = \frac{FP}{FP+TN}$

A. COMPARISON WITH EXISTING DE-AUTHENTICATION SCHEMES

For a rigorous comparison among the key de-authentication solutions, we assess each one of them on a dozen crucial dimensions. TABLE 3 summarizes our comparison and underlines the prominent features and limitations of the key existing solutions.

One of the fundamental requirements for any consumer technology is its user-friendliness. In our context, it is directly related to the unobtrusiveness (cf. col. ①) of a given de-authentication solution and whether it compels the user to carry, wear, or bear anything extra (cf. col. ②). We find that ZEBRA, pulse-response, ZIA, and 1DMRLBP can cause inconvenience to the user by requiring them to bear a bracelet, a pair of electrodes, a token, and an ECG apparatus, respectively. The existing solutions can be further classified as biometric or non-biometric (cf. col. ③) and continuous[10] or non-continuous solutions (cf. col. ④). Biometric-based solutions (i.e., gaze tracking, *Assentication*, pulse-response, keystroke dynamics, BLUFADE, 1DMRLBP) are certainly difficult to evade (cf. col. ⑥) as imitating someone else's biometry or behavioral patterns is highly complex. On the other side, some continuous solutions can be subverted. For instance, authors in the work [29] have shown that an attacker can evade ZEBRA via opportunistic observations. Both the biometric and continuous solutions are accurate. However, the performance of both the categories of solutions comes at the cost of: (1) a user enrollment phase (cf. col. ⑤) that can be laborious and time-consuming for the end-user, and (2) the cost of equipment required to capture their respective features is non-trivial. Only a few solutions are enrollment-free. Regarding the difficulty of evasion, FADEWICH is not suitable for a densely occupied workspace, while the classic timeout approach fails to sense the user's absence.

A user may not interact continuously with her computer (e.g., while attending a phone call). Thus, another key attribute of a user-centric de-authentication scheme is its support for a user's inactivity (cf. col. ⑦). Timeout, ZEBRA, gaze tracking, and keystroke dynamics depend on user interactions, and thus they violate this objective. The main limitation of the majority of existing schemes is their dependence on external equipment for operation (cf. col. ⑧). Such a dependence not only hinders their widespread adoption, but it can also spawn several related concerns, i.e., maintenance, physical customization, deployment complexity, and price. Only timeout approach, keystroke dynamics, BLUFADE, and our proposal do not depend on external hardware; thus, they are not generally affected by the consequent concerns mentioned before.

ZEBRA, DEB, and ZIA demand periodic recharging or replacement of batteries while *Assentication* requires maintenance of the wires that supply power to the chair. The external hardware in the other such solutions is powered directly by the target computer. Finally, all these solutions also involve the risk of physical damage to the external hardware that may seek a replacement (cf. col. ⑨).

Some of the solutions that use external hardware require a particular installation of the equipment (i.e., gaze tracking, DEB) or even customization to workplace infrastructure (i.e., *Assentication*, FADEWICH). The user simply holds/wears the external apparatuses in other such solutions (i.e., ZEBRA, ZIA, 1DMRLBP, pulse-response). As discussed in Section II, BLUFADE requires affixing a particular physical barrier on the webcam (cf. col. ⑩). Regarding deployment complexity (cf. col. ⑪), *Assentication* and FADEWICH are not simple to deploy in practice as they require alteration to infrastructure. Similarly, pulse-response involves complex handling of multiple apparatuses (arbitrary waveform generator, oscilloscope, brass hand-electrode, etc.). All the remaining solutions are simple to deploy even when they need particular placement of hardware (e.g., gaze tracking, DEB, BLUFADE). As far as the price is concerned (cf. col. ⑫), gaze tracking employs an expensive eye-tracking device. Though the price of FADEWICH and pulse-response is unknown, we

[10]The user is re-authenticated throughout the session, and de-authentication happens whenever she cannot prove her identity.

TABLE 3. A comparative summary of the key de-authentication schemes.

⓪	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬
Scheme	**Unobtrusive**	**Nothing to hold**	**Non-biometric**	**Non-continuous authentication**	**Enrollment-free**	**Difficult to evade**	**Inactivity supported**	**No external equipment needed**	**Maintenance-free**	**No particular installation or customization**	**Simple to deploy**	**Price**	**Subjects in user study**
Timeout	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	Low (free)	–
ZEBRA [9]	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	Medium ($100-200)	20
Gaze tracking [1]	✓	✓	✗	✗	✗	✓	✗	✗	✓	✗	✓	High ($2-5k)	30
Assentication [2]	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	Medium ($150)	30
Pulse-response [6]	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	Unknown	10
Keystroke dynamics [19]	✓	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓	Low (free)	33
FADEWICH [7]	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✗	Unknown	3
DEB [8]	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	Low ($10)	15
BLUFADE [12]	✓	✓	✗	✗	✗	✓	✓	✓	✓	✗	✓	Low ($5)	30
ZIA [10]	✗	✗	✓	✗	✗	✓	✓	✗	✗	✓	✓	Low ($10-30)	1
1DMRLBP [11]	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	Medium ($50-200)	–
DEAL (our proposal)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Low (free)	120

suppose they are slightly costlier as they use several sensors and apparatuses. The cost of the remaining schemes is low to medium. Finally, the number of subjects in the user/validation study could indicate the robustness of evaluation results, which is the highest in our case (cf. col. (13)).

In light of our analysis, we find that the state-of-the-art solutions lack a few or several vital characteristics of an effective and practical de-authentication scheme. On the other hand, DEAL is the only solution that possesses all these characteristics. Therefore, we believe it is the most useful and practical de-authentication scheme.

B. LIMITATIONS

We now ponder upon the potential limitations of DEAL.

1) *ALS' presence:* Our proposed de-authentication approach relies on an ALS. While ALS has been present on smartphones and tablets for a long time, it has only recently started to become available on laptops (e.g., MacBooks) and desktops (e.g., iMacs). Therefore, DEAL is futuristic and suitable primarily for newer generations of computers. Nevertheless, one can attach a USB-powered ALS to use DEAL in the absence of a built-in ALS. In particular, DEAL would perform the same as long as an ALS (built-in or externally attached) correctly reports data to it.
One related issue could be the physical placement of ALS on the computer. Any unusual ALS placement (e.g., behind the screen panel) will render our system unusable. In fact, such an unusual ALS placement could be suitable for portable devices, but not for computers that can be docked near a wall. Generally, ALS (like other user-centric sensors, e.g., webcam) is mounted on the front side of the display screen. Our approach will work as long as ALS faces the users. For the sake of readers' convenience, FIGURE 1 and FIGURE 6 conceptualize DEAL on a laptop and a desktop, respectively.

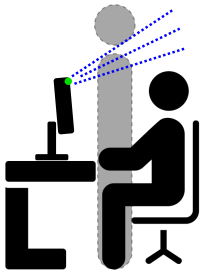


FIGURE 6. A representative conceptualization of DEAL on a desktop.

2) *False alarms due to passersby:* A common phenomenon in any workplace setting is the movements of passersby (e.g., colleagues). We set up a separate experiment to investigate such a scenario. FIGURE 7 shows different user positions, where (A) represents the legitimate user's standing position, (B) shows a passerby crossing too close to the target user, and (C) depicts a passerby away from the target user.

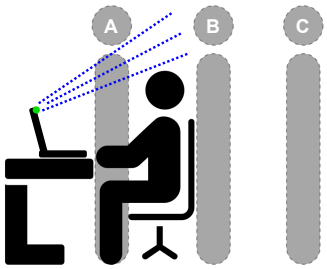


FIGURE 7. An illustration of passersby near our user's work-desk.

We find that our system remains largely unaffected as long as a passerby (cf. (C)) walks at about 2-3 ft distance from the user. In particular, any wave of outliers, if induced, is sparse and short. On the other hand, our system de-authenticates the user when a passerby (cf. (B)) comes too close to the user; as it affects the ALS readings. It can be seen as a false alarm. Nevertheless, such de-authentications can protect the user's privacy from shoulder surfers and onlookers.

3) *Violation of our assumptions:* Our system will create a false alarm if the user changes her working posture (e.g., from sitting to standing). Similarly, it may possibly not de-authenticate the user if she moves away from her work-desk without getting up (e.g., by dragging the chair). Violating the assumptions or requirements of any given scheme will affect its functioning, and our work is no different.

VII. CONCLUSION AND FUTURE WORK

Both user authentication and de-authentication are essential operations for the security of a computer system. It is even more critical to de-authenticate a user in a shared workspace setting because an insider can gain access to the user's active session through *lunchtime* attacks. The research community has proposed different de-authentication and continuous-authentication techniques over the inactivity timeout-based method. The existing works unfortunately have various limitations, e.g., complex installation procedures, requirement of external hardware to assert user presence. In this paper, we propose a novel approach, called DEAL, that uses ALS present on a computer to de-authenticate the user. We assessed the quality of our proposed approach empirically in the real world. While being effective and fast, DEAL is also unobtrusive.

In the future, we would like to test DEAL in unconventional workplace settings, such as in a cafe or under different colored lighting. We will explore the possibility of assisting DEAL with machine learning-based classification techniques to further improve its performance. We will also investigate the effect of personalized tuning (e.g., via an enrollment stage for the end user) on its performance.

IRB APPROVAL

We obtained prior approval for our experiments from the Institutional Review Board (IRB) of the institute, where the experiments were carried out. The level of review recommendation was: *Exempt.* All participants were volunteers, who were informed of the actual use of the collected data, and their informed consent was obtained before starting the data collection process. No sensitive data was collected. In particular, no participant names, contact numbers, or other Personally Identifying Information (PII) was collected. The minimal identifying information retained was also anonymized. All the data was (and is) stored in an encrypted form.

REFERENCES

[1] Simon Eberz, K Rasmussen, Vincent Lenders, and Ivan Martinovic. Preventing Lunchtime Attacks: Fighting Insider Threats with Eye Movement Biometrics. In *NDSS*, pages 1–13, 2015.

[2] Tyler Kaczmarek, Ercan Ozturk, and Gene Tsudik. *Assentication*: User De-authentication and Lunchtime Attack Mitigation with Seated Posture Biometric. In *ACNS*, pages 616–633, 2018.

[3] Sara Sinclair and Sean W Smith. Preventative Directions for Insider Threat Mitigation via Access Control. In *Springer Insider Attack and Cyber Security*, pages 165–194. 2008.

[4] Xuerui Wang, Zheng Yan, Rui Zhang, and Peng Zhang. Attacks and Defenses in User Authentication Systems: A Survey. *Elsevier JNCA*, 188:103080, 2021.

[5] Dario Pasquini, Ankit Gangwal, Giuseppe Ateniese, Massimo Bernaschi, and Mauro Conti. Improving Password Guessing via Representation Learning. In *IEEE S&P*, pages 1382–1399, 2021.

[6] Kasper Bonne Rasmussen, Marc Roeschlin, Ivan Martinovic, and Gene Tsudik. Authentication using Pulse-Response Biometrics. In *NDSS*, pages 1–14, 2014.

[7] Mauro Conti, Giulio Lovisotto, Ivan Martinovic, and Gene Tsudik. FADEWICH: Fast Deauthentication over the Wireless Channel. In *ICDCS*, pages 2294–2301, 2017.

[8] Mauro Conti, Pier Paolo Tricomi, and Gene Tsudik. DE-auth of the Blue! Transparent De-authentication using Bluetooth Low Energy Beacon. In *ESORICS*, pages 277–294, 2020.

[9] Shrirang Mare, Andrés Molina Markham, Cory Cornelius, Ronald Peterson, and David Kotz. ZEBRA: Zero-effort Bilateral Recurring Authentication. In *IEEE S&P*, pages 705–720, 2014.

[10] Mark D Corner and Brian D Noble. Zero-Interaction Authentication. In *MobiCom*, pages 1–11, 2002.

[11] Wael Louis, Majid Komeili, and Dimitrios Hatzinakos. Continuous Authentication using One-dimensional Multi-resolution Local Binary Patterns (1DMRLBP) In ECG Biometrics. *IEEE TIFS*, 11(12):2818–2832, 2016.

[12] Matteo Cardaioli, Mauro Conti, Pier Paolo Tricomi, and Gene Tsudik. Privacy-Friendly De-authentication with BLUFADE: Blurred Face Detection. In *IEEE PerCom*, pages 197–206, 2022.

[13] The College of Optometrists. Screen Use. https://lookafteryoureyes.org/eye-care/screen-use/, 2023.

[14] Md Hajian Berenjestanaki, Mauro Conti, and Ankit Gangwal. On the Exploitation of Online SMS Receiving Services to Forge ID Verification. In *ARES*, pages 1–5, 2019.

[15] Salil P Banerjee and Damon L Woodard. Biometric Authentication and Identification using Keystroke Dynamics: A Survey. *Journal of Pattern Recognition Research*, 7(1):116–139, 2012.

[16] Tomi Kinnunen, Filip Sedlak, and Roman Bednarik. Towards Task-independent Person Authentication using Eye Movement Signals. In *ACM ETRA*, pages 187–190, 2010.

[17] Joseph Bonneau. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *IEEE S&P*, pages 538–552, 2012.

[18] Committee on National Security Systems. Report No. 4009, March 2022.

[19] Rick Joyce and Gopal Gupta. Identity Authentication based on Keystroke Latencies. *Communications of the ACM*, 33(2):168–176, 1990.

[20] Chee Meng Tey, Payas Gupta, and Debin Gao. I Can Be You: Questioning the Use of Keystroke Dynamics as Biometrics. In *NDSS*, pages 1–16, 2013.

[21] HP. The HP Webcam Survey. https://press.hp.com/us/en/press-kits/2019/the-hp-webcam-survey.html, 2019.

[22] Hyoseok Yoon, Se-Ho Park, and Kyung-Taek Lee. Exploiting Ambient Light Sensor for Authentication on Wearable Devices. In *IEEE CyberSec*, pages 95–100, 2015.

[23] Ashton Holmes, Sunny Desai, and Ani Nahapetian. LuxLeak: Capturing Computing Activity using Smart Device Ambient Light Sensors. In *SmartObjects Workshop*, pages 47–52, 2016.

[24] Valeriu Manuel Ionescu. Exploiting the Ambient Light Sensor to Track User Environment Information. In *IEEE RoEduNet*, pages 1–6, 2016.

[25] Raphael Spreitzer. PIN Skimming: Exploiting the Ambient Light Sensor in Mobile Devices. In *ACM SPSM Workshop*, pages 51–62, 2014.

[26] Jiacheng Shang and Jie Wu. LightDefender: Protecting PIN Input using Ambient Light Sensor. In *IEEE PerCom*, pages 1–10, 2020.

[27] Bastien Nocera. iio-sensor-proxy. https://gitlab.freedesktop.org/hadess/iio-sensor-proxy/, 2022.

[28] Max Roser, Cameron Appel, and Hannah Ritchie. Human Height. https://ourworldindata.org/human-height, 2019.

[29] Otto Huhta, Prakash Shrestha, Swapnil Udar, Mika Juuti, Nitesh Saxena, and N Asokan. Pitfalls in Designing Zero-effort Deauthentication: Opportunistic Human Observation Attacks. In *NDSS*, pages 1–14, 2016.

ANKIT GANGWAL is an Assistant Professor at International Institute of Information Technology (IIIT) Hyderabad, India. Prior to joining IIIT Hyderabad, he was a Post-Doctoral Researcher at TU Delft, Netherlands. He received his Ph.D. degree from University of Padova, Italy, in 2020. His main research interest is in the area of cybersecurity.

AASHISH PALIWAL is a doctoral student at IIIT Hyderabad working in the Centre for Security, Theory, and Algorithmic Research. He has previously worked at NPCI's Blockchain Centre of Excellence. His current research area includes security, blockchain, and payment systems.

MAURO CONTI (Fellow, IEEE) received the Ph.D. degree from the Sapienza University of Rome, Italy, in 2009. After the Ph.D. degree, he was a Postdoctoral Researcher with Vrije Universiteit Amsterdam, The Netherlands. In 2011, he joined as an Assistant Professor with the University of Padua, where he became an Associate Professor, in 2015, and then a Professor, in 2018. He was a Visiting Researcher with GMU, in 2008 and 2016, UCLA, in 2010, UCI, in 2012, 2013, 2014, and 2017, TU Darmstadt, in 2013, UF, in 2015, and FIU, in 2015 and 2016. He is currently a Professor with the University of Padua, Italy, and an affiliate Professor with the University of Washington. His research interests include security and privacy. In this areas, he has published more than 200 papers in the topmost international peer-reviewed journals and conferences.