IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 8, 2020, accepted April 18, 2020, date of publication April 27, 2020, date of current version May 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2990604

0EISUA: Zero Effort Indoor Secure User Authentication

ALI ABDULLAH S. ALQAHTANI[1], (Student Member, IEEE), HOSAM ALAMLEH[2], AND JEAN GOURD[3], (Member, IEEE)

[1]Department of Cyberspace Engineering, Louisiana Tech University, Ruston, LA 71270, USA
[2]Department of Computing and Information Science, Edgewood College, Madison, WI 53713, USA
[3]Department of Cyber Engineering and Computer Science, Louisiana Tech University, Ruston, LA 71270, USA

Corresponding author: Ali Abdullah S. AlQahtani (alqahtani.aasa@gmail.com)

This article was funded by Louisiana Tech University.

ABSTRACT Two-factor authentication (2FA) systems implement by verifying at least two factors. A factor can be one or more of something a user knows (password, or phrase), something a user possesses (smart card, or smartphone), something a user is (fingerprint, or iris), something a user does (keystroke), or somewhere a user is (location). In a conventional 2FA system, a user is required to interacts (e.g., typing a passcode) in order to implement the second layer of authentication, which is not very user-friendly. Nowadays, smart devices (phones, laptops, tablets, etc.) can receive signals from different radio frequency technologies within range. As these devices move among networks (Wi-Fi access points, cell phone towers, etc.), they receive broadcast messages, some of which can be used to collect information. This information can be utilized in a variety of ways, such as establishing a connection, sharing information, locating devices, and, most appropriately, identifying users in range. The principal benefit of broadcast messages is that the devices can read and process the embedded information without being connected to the broadcaster. Moreover, the broadcast messages can be received only within a range of the wireless access point sending the broadcast, thus inherently limiting access to those devices in close physical proximity and facilitating many applications dependent on that proximity. In this paper, 0EISUA is proposed, a zero-effort two-factor authentication scheme based on something that is in the user's environment (ambient access points). In our research, data from the broadcast messages are utilized to implement the second authentication factor by determining whether two devices are proximate or not to ensure that they belong to the same user, in a way that requires zero interaction from the user. The new proposed system introduced in this paper is experimentally tested.

INDEX TERMS Two-factor authentication, trilateration system, sound ambient, ambient access points, zero effort, 0EISUA, RSSI, NFC, OTP, QR.

I. INTRODUCTION

User authentication is considered as a critical factor in the first layer of security that establishes confidence in user identities when presented to an information system. Traditionally, passwords and personal identification numbers (PIN) are used to protect information. However, some users keep the same password for multiple accounts [2]. Besides, some users allow the browser to save their passwords, making their accounts more vulnerable [2]. Moreover, password authentication is prone to many types of attacks such as dictionary attacks, brute force attacks, traffic interception, the man in the middle attacks, keylogger attacks, social engineering attacks, and thwarting password attacks [1].

Two-factor authentication (2FA) is a secure technique that requires two levels of security to authenticate a user to ensure the security of the user, even if a password is compromised.

As cyber-attacks have evolved, a diverse set of authentication methods have been developed to be able to fight back against the evolved cyber-attack. The most common authentication methods fall into two categories: Single-Factor Authentication (SFA) and Two-Factor Authentication (2FA). A factor can be considered one of the following: somewhere a user is, something a user possesses, something a user is, something a user knows, or something a user does. These five elements are called authentication credentials.

The associate editor coordinating the review of this manuscript and approving it for publication was S. K. Hafizul Islam.

A. SOMETHING A USER KNOWS

When a user logs into an information system, the first task involves identification. Identification can be done by typing in a username, for example. In order to authenticate a client, the client must prove that he/she is the actual owner of an existing profile. This step could be done by providing something no one but that user knows – such as a password.

Currently, passwords are the most common category of authentication. Nevertheless, only depending on a password to protect data is often considered a weak form of protection. Moreover, there are numerous types of attacks that target ‘‘something a user knows’’ such as brute force, dictionary, and keylogger attacks. In response to these attacks, users should take some actions to strengthen passwords. To highly secure a user's information, passwords should be unique and contain upper- and lower-case letters, numbers, and special characters.

B. SOMETHING A USER POSSESSES

This category of authentication is based on items that a user physically possesses. These items are used along with passwords. Due to the usage of two types of authentication, what a user knows (a password) and what the user has, this type of authentication is usually referred to as Two-factor Authentication (2FA). However, if a user were to use one without the other, it would be considered as Single-factor Authentication (SFA). Nowadays, the common items used to authenticate users are Tokens, Smart Cards, and Smartphones.

C. SOMETHING A USER IS

This type of authentication depends on the features and characteristics of a human. These features and characteristics can either be physical or abstract. This form of authentication is known as biometric authentication. Physical biometric authentication is called Standard Biometrics and an unphysical biometric authentication is called Cognitive Biometrics.

D. SOMETHING A USER DOES

It is another style of security that is based on identifying and measuring patterns based on a person's behavior while performing certain activities. This kind of authentication is known as behavioral biometrics. Keystroke dynamics and voice recognition are two examples of behavioral biometrics.

E. SOMEWHERE A USER IS

This type of authentication is based on a user's location, which is known as geolocation. The location might not be considered as a unique identifier to a user. However, it can be utilized to indicate if a remote adversary is attempting to perform some sort of malicious activity from a location that is not the normal location of the user.

To sum up, we have mentioned the five elements of authentication, which are called authentication credentials. These five elements are somewhere a user is, something a user possesses, something a user is, something a user knows, and something a user does. Our goal is to add a second layer of authentication utilizing the current IEEE 802.11 infrastructure to prove a user's identity without adding any extra burden on users.

In the next section, some existing researches in the field of 2FA are discussed. In part A, B, and C, the schemes that require extra effort from users in the authentication phase are discussed. However, part D discusses research that requires zero effort in the authentication phase.

II. LITERATURE REVIEW

This section provides an overview of the notable literature published on the topic of 2FA that is relevant to our work.

A. ONE-TIME PASSWORD (OTP)

OTP is utilized as an authentication scheme whereby an OTP password is obtained through a user's smartphone. In [8], Eldefrawy, Alghathbar, and Khan proposed a protocol banking system that is OTP-based using a mobile phone, which is based on the infinite hash chain. A user in the registration phase gets two different hash functions and initial seed to establish on a user's mobile devices. When a user logs in, the system server will get the user has chain status to synchronize the server's has chain with the use hash chain with the same value. Then the server responds with an OTP's and waits for the user to enter it and sends it back to the server. The server side compares the received OTP with the one that has been generated by the server. Based on the outcome, the server decides to either authorize or reject the user. The weakness inherent to this method: [8] specifically, the hash chain is infinite; therefore, when the login times becomes too large, the server's computational cost will be too heavy and will take some time until a user gains access [13]. Also, the authentication is one-way authentication, which means that the server is always trusted; therefore, this system is vulnerable to phishing attacks. However, the major security threat is that there a possible disclosure of the encrypted OTP list from the user's side [8], [9]. Also, the system uses a strong encryption method (i.e., Twofish), but there is still a weakness in that an attacker could decrypt the OTP during its period of validity [8]. The personal identifying information must be written on a form and mailed to the server's operator, which, during transit, might be exposed to postal workers or be stolen by a third party [10]. Besides, the user is required to verbally read the oath message, which could be on an unencrypted line that might cause a user's voiceprint to be recorded and subsequently used by an attacker.

B. QUICK RESPONSE CODES (QR)

QR technology is used, where an authentication server generates a QR code. On the client-side, a user must scan it with his/her smartphone using a relevant application. A scheme was proposed by Rodrigues *et al.* [11]. It uses QR technology to create a 2nd Factor. In order to create a user's profile and store it in the system, a user must first visit a remote server (usually a website) and submit their full name, email address, password, and the International Mobile Equipment Identity (IMEI) of their mobile phone. Subsequently, the remote server generates a QR code using the

IMEI information and random four-digit code. The user then uses a special app installed on their mobile phone to scan the QR code and inputs the received string into the remote server to verify the information and complete the registration phase. To later authenticate, the user performs the same QR code-scan and string-input procedure. If the entered string from the scanned QR code matches the information on the server, the user will gain access. A significant weakness in this method involves the possibility of spoofing an IMEI at either the hardware, the OS, or even the application level. Moreover, there is also the problem of interception, as the QR code will be displayed on the user's screen during the entire authentication process, which can be copied from a distance [12]. Possibly, a user might be subjected to an impersonation attack where an attacker steals the QR code from the screen [13]. Through the exposed QR code, the attacker could possibly obtain the user's IMEI and impersonate the user via spoofing. This would be difficult to discover and rectify in a timely manner [14].

C. NEAR FIELD COMMUNICATION (NFC)

NFC technology has been used as a method to authenticate users. In these methods, a user must get an NFC tag close enough to an NFC reader. Hufstetler, Ramos, and Wang proposed a 2FA system that works by scanning an authorized NFC tag [15]. The method relies on pGina, an open-source credential provider replacement allowing developers to create plugins for new modes of authentication and authorization. Moreover, an NFC tag needs to be attached to the user's system and configured with pGina. During login, the user is asked to type in a predefined passcode into a pGina login page. When ready, the user clicks the login button while simultaneously holding an authorized NFC tag up to the reader. The entered information and the scanned NFC tag are sent to the plugin to check if they match the ones registered during setup. Depending on the outcome, pGina will either deny the user or grant access to the remote system. There are several weaknesses with this approach that are largely due to the wireless nature of NFC [5]. Eavesdropping can occur during NFC communication if the attacker is close enough to the user's device [14], [15]. NFC does not have any type of guard against the possibility of eavesdropping [16]. Also, since every NFC tag has a built-in unique ID, this ID could be spoofed, captured, or copied as the ID is not encrypted, meaning that it might not be enough to protect user-information [4], [17].

D. AMBIENT SOUND

QuickAuth, SoundAuth, and Sound-Proof are authentication systems that utilize ambient sound to authenticate users [1], [6]. These systems validate users by comparing ambient sounds that have been recorded by both authentication devices (e.g., a smartphone, a computer, etc.) to determine if both devices are co-located. Wang, Zhu, Yan, and Wang published a system, called Sound Auth, which generates random, near-ultrasounds for more accurate comparison [6]. Similarly, a user initiates a login request to a remote server, and both devices begin recording. In this method, both background noise and near-ultrasounds that are generated by the user's web browser are recorded for the duration of the login procedure. When recording is completed, each device sends back the recorded audio to the server for comparison and to determine whether to accept or deny access during authentication. This system, however, might not fit all environments because it depends on the ability to listen to ambient sound. Not all devices are equipped with a built-in microphone. The user may also be unable to find an environment with the right noise levels appropriate to the software when needed [3], [4]. If there is a single loud source of noise, such as a television playing in the background, construction, or music, it may also be possible to trick the system into thinking the mobile device is in the same location as the authentication device [5]. The possibility of "overhearing" important, private information can lead to significant security vulnerabilities or infringe on the privacy of users [1].

Our proposed system utilizes IEEE 802.11 (Wi-Fi) as the medium for its ubiquity. The proposed model is unique in that it grants access only when the two devices are in the same general vicinity and near enough each other. This feature allows the new system to remove the "weak link" from the 2FA, which usually takes the form of human patience and attention. The proposed system allows a user to log in with the benefits of 2FA, but without the normal hassle involved with a pin, phrase, or physical key based 2nd factor.

III. SYSTEM MODEL

The difference between 0EISUA and traditional 2FA approaches is that the first authentication factor in 0EISUA is credential information. Moreover, custom smartphone and desktop applications, which must be installed on participating devices in the registration stage. 0EISUA is a zero-effort 2FA system that means the second-factor authentication requires zero interaction (i.e., the user is only required to enter the primary credentials such as username and password). The proposed model depends on something that is in the user's environment. The 2FA step of 0EISUA is the proximity of a smartphone to a login device (such as a desktop) which a user uses to log into the 0EISUA service. A decision to either grant or deny access takes place, where the 0EISUA service verifies that both devices are in the same location, and the distance between them is within a predefined (acceptable) range. 0EISUA utilizes Received Signal Strength Indicator (RSSI) values to calculate the distance between a user's devices. It is well known that RSSI tends to fluctuate, which makes it difficult to be spoofed by attackers.

A. 0EISUA ARCHITECTURE

The proposed system architecture consists of:

a) Participating devices: an authentication device (e.g., smartphone) and a login machine (e.g., computer), which are assumed to be Wi-Fi-capable devices.

b) Relevant applications: The relevant applications must be installed on the participating devices. Since the system is intended to be zero-interaction on the part of users, the mobile application automatically launches and handles the login process on the mobile device. Both applications automatically scan and collect data from surrounding Wi-Fi access points and subsequently send the collected data to the 0EISUA subsystem on the 0EISUA server.

c) A server: In the proposed system, the server can be remote or local as wanted. The 0EISUA server uses data received from participating devices and determines if they are co-located and within a predefined acceptable distance from each other.

As can be seen from the architecture, the proposed system is zero effort because the collection, sending, and the verifying of data of surrounding Wi-Fi access points happen in the background without any user involvement.

B. 0EISUA DESIGN

The proposed system is a type of access control system. Access control is a security technique that provides access to a place or a source based on selective restrictions that have been described by an administration. As an access control system, 0EISUA will handle identification, authentication, and authorization.

The identification phase can be done by requiring a user to type in a username that will be used as the means by which users are identified. Also, the desktop and smartphone applications. Authentication can be achieved when a user further provides a correct password (i.e., one that is associated with the provided username). Authorization is an act that validates data according to a predefined mechanism and based on the result, either gives permission or not. Here, it will be performed by 0EISUA's server that compares the information received from two devices: the one used to attempt the login with the 0EISUA service, and the user's pre-registered mobile device.

C. 0EISUA OPERATION

In this section, the operation of 0EISUA that contains two phases is described.

1) REGISTRATION PHASE

In this phase, a user must create an account in the 0EISUA server Figure 1. Then the user receives the 0EISUA applications for installation on the two devices Figure 2, Figure 3. After installing the 0EISUA applications, the user account is activated by logging into the mobile application Figure 4.

2) LOGIN AND AUTHENTICATION PHASE

This section will show the login and authentication procedures between a user and the 0EISUA server. The steps are shown in Figure 5.

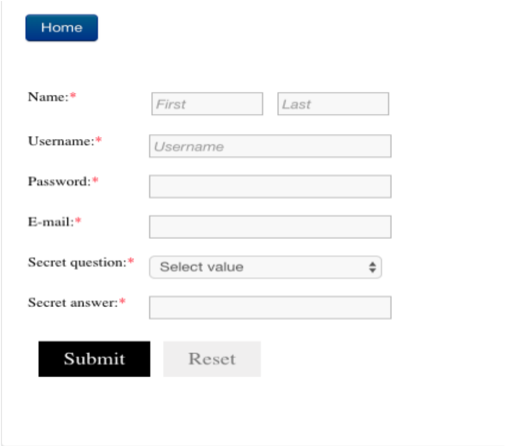


FIGURE 1. **Registration page.**

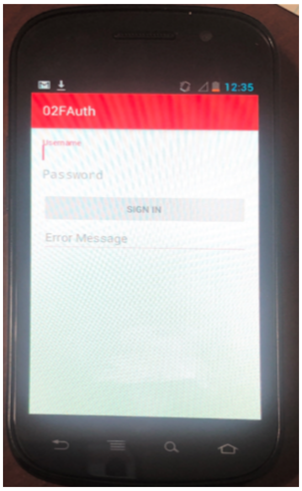


FIGURE 2. **Mobile application.**

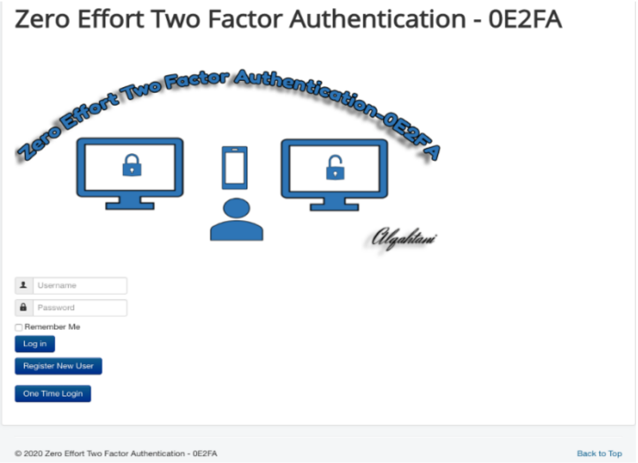

Zero Effort Two Factor Authentication - 0E2FA
Zero Effort Two Factor Authentication-0E2FA
Alqahtani
Username
Password
□ Remember Me
Log in
Register New User
One Time Login
© 2020 Zero Effort Two Factor Authentication - 0E2FA
Back to Top

FIGURE 3. **Desktop application.**

1) A user submits login credentials to the 0EISUA server from the login device.

2) The server sends a request to the desktop and mobile devices to scan the three access points' beacon frames.

Your account is now active

FIGURE 4. Account activation.

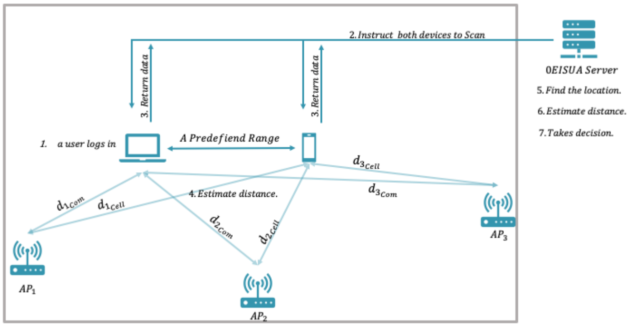


FIGURE 5. 0EISUA overview.

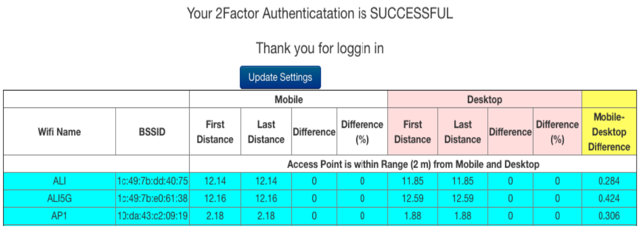
3) Both devices send the requested information (SSID, BSSID, RSSI values) back to the 0EISUA server.
4) The RSSI values are used with equation (1) to estimate the distance between each device to each of the access points.

$$PL_{log} = PL_0 + 10\gamma log_{10}\frac{d}{d_0} \tag{1}$$

where PL_{log} is the transmitted power is minus the received power, PL_0 is the path loss in dB, λ is the operating wavelength, γ is the path loss exponent, and d_0 is the reference distance (1m).
5) The estimated distance is used to find the location of each device by implementing the logic in equation (2).

$$\left.\begin{aligned}(x-x_1)^2+(y-y_1)^2 &= d_1^2\\(x-x_2)^2+(y-y_2)^2 &= d_2^2\\(x-x_3)^2+(y-y_3)^2 &= d_3^2\end{aligned}\right\} \tag{2}$$

equation (2) is the formula that is used to determine the location in trilateration systems.
6) Based on the results of step 5, the distance between the two devices is estimated.
7) The system decides whether to allow or deny access based on the distance between the two devices if they are within predefined acceptable range access is granted; otherwise access is denied.

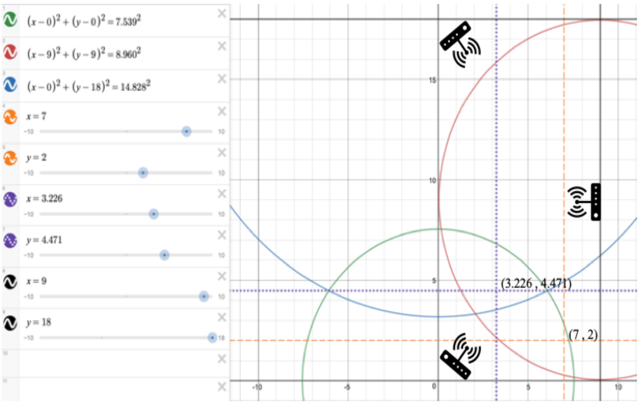


Your 2Factor Authenticatation is SUCCESSFUL

Thank you for loggin in

		Mobile				Desktop				
Wifi Name	BSSID	First Distance	Last Distance	Difference	Difference (%)	First Distance	Last Distance	Difference	Difference (%)	Mobile-Desktop Difference
		Access Point is within Range (2 m) from Mobile and Desktop								
ALI	1c:49:7b:dd:40:75	12.14	12.14	0	0	11.85	11.85	0	0	0.284
ALI5G	1c:49:7b:e0:61:38	12.16	12.16	0	0	12.59	12.59	0	0	0.424
AP1	10:da:43:c2:09:19	2.18	2.18	0	0	1.88	1.88	0	0	0.306

FIGURE 6. Authentication page.


$(x-0)^2+(y-0)^2=7.539^2$

$(x-9)^2+(y-9)^2=8.960^2$

$(x-0)^2+(y-18)^2=14.828^2$

$x=7$

$y=2$

$x=3.226$

$y=4.471$

$x=9$

$y=18$

FIGURE 7. Location accuracy experiment.

IV. EXPERIMENT

This section describes our experimental setup and discusses the multiple experiments that were conducted to test the operation of the proposed system. A smartphone and a desktop applications were developed to implement the 0EISUA model. The applications respond to a request from the 0EISUA server and scans all the three access points. The mobile device communicates with the server either via a cellular network or Wi-Fi, while the computer connects to the 0EISUA server over Wi-Fi or an Ethernet connection.

A. LOCATION ACCURACY

In this experiment, we used three access points at different locations in a room. Two access points were placed at the two corners of the room, while the third one was placed at the center wall that was adjacent to the two access points, as can be seen in Figure 7 below. The exact positions of the three access points were measured and located manually on the study site as a preliminary step. Subsequently, seven different actual locations were calculated. A device was located at each position then scanned the three Wi-Fi access points' beacon frames along with their corresponding RSSI values. Figure 7 shows the result of this experiment, comparing the actual location of the user's devices with the calculated location.

TABLE 1. Experiment one (average).

Actual points	Calculated points	Difference in feet
(2 , 17)	(5.173 , 15.424)	3.543 ft
(3 , 2)	(1.443 , 7.478)	5.695 ft
(4.5 , 9)	(3.893 , 9.869)	1.060 ft
(5 , 14)	(4.007 , 12.636)	1.687 ft
(6 , 2)	(6.968 , 2.361)	1.033 ft
(7 , 2)	(3.226 , 4.471)	4.511 ft
(8 , 16)	(5.173 , 15.424)	3.543 ft

TABLE 2. Experiment two (median).

Actual points	Calculated points	Difference in feet
(2 , 17)	(5.591 , 15.842)	3.773 ft
(3 , 2)	(1.484 , 7.516)	5.721ft
(4.5 , 9)	(3.893, 9.869)	1.06 ft
(5 , 14)	(3.957, 12.612)	1.737 ft
(6 , 2)	(6.827 , 2.606)	1.025 ft
(7 , 2)	(4.332 , 3.438)	3.031ft
(8 , 16)	(5.392 , 10.249)	6.315 ft

1) EXPERIMENT NO. 1

The system scanned the RSSI value 30 times from 7 different points. Then obtained the average to calculate the location using equations (1) and (2). The results are shown in Table 1.

2) EXPERIMENT NO. 2

The system scanned the RSSI value 30 times from 7 different points. Then obtained the median to calculate the location using equations (1), and (2). The results are shown in Table 2.

Table 1 and Table 2 show the comparison between the true location of the devices versus the locations calculated by the proposed system for each case (the average and median of RSSI values). As can be seen from the results, there is no major difference between an actual location and the calculated location. The system achieves satisfactory results.

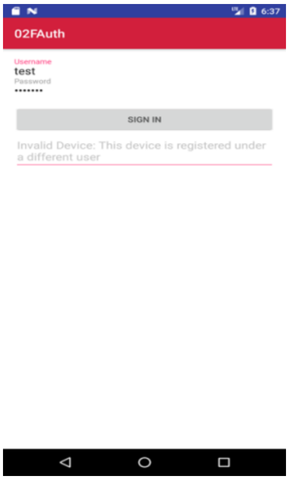
B. AUTHENTICATION SUCCESS RATE

In this experiment, a user's devices were placed at each position of the seven different actual positions. Then the user's devices scanned the three Wi-Fi access points' beacon frames along with their corresponding RSSI for 30 times at each point. The authentication success rate of the proposed system was evaluated by calculating the distance between the two devices if the distance between them is 2 meters or less access is granted; otherwise, access is denied. The results are shown in the confusion matrix in Table 3. Finally, the proposed system performance rate accuracy was calculated using the data from Table 3 and by plugging it into equation (3). At best, the proposed system provides a 93.3% authentication accuracy rate.

$$\frac{True\ Positive + True\ Negative}{N,\ Total\ number\ of\ a\ dataset} \times 100 \qquad (3)$$

TABLE 3. Authentication success rare.

N = 210		Actual	
		Positive	Negative
Predicted	True	100	6
	False	8	96



Username
test
Password
•••••••

Invalid Device: This device is registered under a different user

FIGURE 8. Mobile application rejection.

TABLE 4. Testing different models between phones.

Phone Model	Number of Reading	Min	Mix	Average	StdDev
S9	1000	-58	-45	-50.07	2.19
OnePlus 3	1000	-59	-48	-50.97	2.14
Samsung S4	1000	-60	-50	-52.31	1.75
Motorola Moto Z	1000	-57	-49	-51.74	2.00
All Phones	4000	-60	-45	-51.27	2.19

C. MOBILE APPLICATION SECURITY

In this experiment, the security of the 0EISUA mobile application was examined and tested. We attempted to log in with credential information of an account that was not associated with the smartphone application. As can be seen in Figure 8 below, the application rejected the request. This feature addresses the potential scenario that if an attacker gets or installs the client-side application, the attacker cannot communicate with the 0EISUA server even if he/she knows the username and password of a user.

D. TESTING DIFFERENT MODELS BETWEEN PHONES

In this experiment, four different models of smartphones were placed next to each other. RSSI data was collected for an access point in range by the four smartphones using a smartphone application, Figure 9. The results are shown in Table 4.

As can be observed from the results proved consistent with respect to RSSI values measured across different smartphones. This is due to the fact that the internal omnidirectional antennas of mobile phones are necessarily

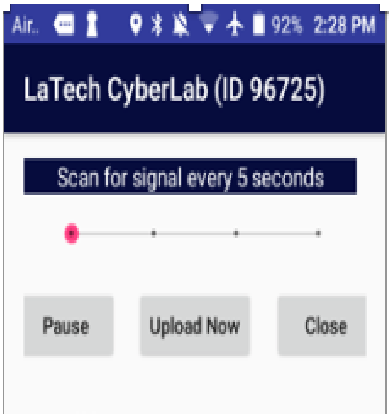


FIGURE 9. Mobile application.

TABLE 5. Duration time in seconds.

Attempts	Average	Minimum	Maximum	Standard Deviation
50	8.77	5.98	16.29	1.96

small. Thus, the gain value of small omnidirectional antennas is theoretically limited [19], and in practice does not exceed 5 dB. Gain values of 2 dB or 3 dB are common. Moreover, the Federal Communications Commission (FCC) has limits on Wi-Fi antennas gains [20]. This combines to effectively assure similar RSSI readings across typical mobile devices used by users in the proposed system.

E. COMPUTATION AND COMMUNICATION ANALYSIS

The goal of this experiment is to calculate the time interval between releasing a login button and delivering a decision. In this experiment, a user logged in 50 times one after another and for each case, the time duration was counted. As can be seen in Table 5, the system achieved superior results during the 50 attempts.

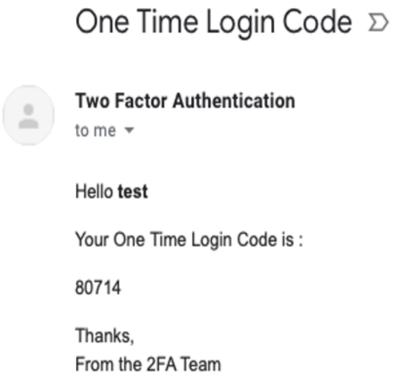
F. ABSENCE OF THE AUTHENTICATION DEVICE

The authentication device is a smartphone that has the 0EISUA mobile application installed on it. In the case were a user does not have the authentication device for any reason, such as the device was forgotten, lost, or stolen. The proposed system handles this issue, where the user can use a One-time Login feature. For this feature, the user types in a username and answers the security question, then an OTP is sent to the registered email, which can be used to access the authorization entity Figure 10.

In this section, several experiments have been implemented. From the results, we believe that the proposed system is an efficient method to establish a zero effort 2FA scheme.

V. SYSTEM ANALYSIS

In this section, the different aspects of the proposed system are evaluated based on the experiments performed. Moreover, the various factors and parameters that play a role in the proposed system's performance are analyzed.


One Time Login Code

Two Factor Authentication
to me

Hello **test**

Your One Time Login Code is :

80714

Thanks,
From the 2FA Team

FIGURE 10. OTLC.

Section A discusses the proposed system's security aspect. Section B examines the response to diverse types of attacks. Section C evaluates how convenient the system is for a user. Section D is a review of the proposed system's cost.

A. SECURITY

To enhance the security of the system, we chose to implement 2FA as a solution if a user's password is compromised, we can ensure that the security of a user remains with at least two levels of authentication. Furthermore, this research aims to add an extra layer of authentication by finding something unique in a user's environment – specifically, by utilizing information in ambient access points. In this section, we analyzed the features of the proposed system, followed by several types of anticipated attacks and how the proposed system responds to each one.

1) 0EISUA APPLICATIONS

To ensure client-side security, the 0EISUA applications cannot be found on any public source (i.e., App Store, Play Store, etc.). The client-side applications can only be obtained through the 0EISUA's server. This feature limits access to the applications to registered and fully authenticated users. The smartphone application must be secured by associating it with the mobile device's IMEI and another unique identifier of the smartphone (e.g., device ID, serial number, or with both if needed). The desktop application must be secured by associating it with the desktop UUID and another unique identifier of the PC if needed. Without either of the applications, a user cannot use the 0EISUA scheme effectively. However, we might consider that it is not convenient for the user to install them on their devices, but with the applications, accessing the system is limited and the security is increased. The users must have both to be able to use the 0EISUA scheme.

2) BEACON FRAME

The Proposed scheme is designed to be a zero effort 2FA system that uses the signals broadcast by Wi-Fi access points as the second level of security without the need for user intervention. Each access point periodically broadcasts a unique

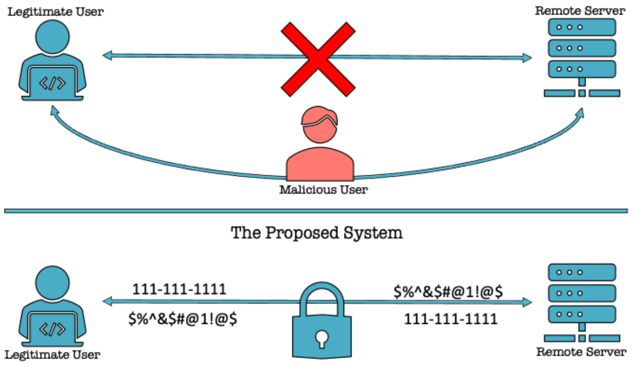


FIGURE 11. The man-in-the-middle attack.

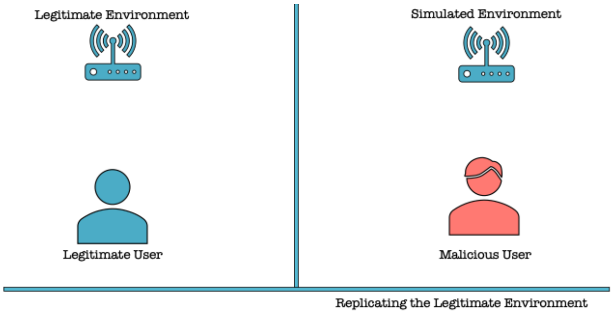


FIGURE 12. Simulate the user's environment.

beacon frame to all devices in range. The significant benefit of this is that the beacon frames can be received while only within a limited physical range of each wireless access point, therefore limiting the potential for spoofing or impersonation, making the 2nd factor more secure. 0EISUA utilizes the RSSI value to calculate the distance from the transmitter (access points) to each receiver (user's smartphone and desktop). Furthermore, using the RSSI value as a means to measure the user's location, can help to ensure that the user is within a limited physical range of each access point that is scanned, and further decreasing the chances of spoofing or impersonation.

3) THE SECOND LAYER OF AUTHENTICATION

The 0EISUA system is designed to be secure and different from the traditional 2FA approaches. The first layer of authentication is something a client knows, a password. Moreover, the relevant smartphone and desktop applications. The second layer of authentication is something unique in the client's environment, beacon frames. Without requiring any interaction from the user, we can authenticate and authorize access. the user gains access if the two devices meet the following characteristic:

a) Existing in a range of all the predefined access points.
b) Both devices must detect all the predefined access points in the time of authentication.
c) The estimated distance between the two devices falls within a predefined range.

B. CYBER-ATTACK VULNERABILITY ASSESSMENT

In the proposed system's vulnerability for some of the common cyber-attacks are assessed and discussed. These cyber-attacks were chosen by analyzing the possible threats to our proposed method and its components. Furthermore, the steps taken to minimize threats from these types of attacks are also discussed.

1) THE MAN-IN-THE-MIDDLE ATTACK

The man-in-the-middle attack occurs when an attacker is inserted in the system and secretly intercepts communication occurring within the system Figure 11. Often, such an attacker transmits (and possibly even alters) communication between two parties who believe that they are directly communicating with each other. This result is the appearance of normal communication between the two parties. In our experiments, the SSL protocol is utilized for communicating between a user's devices and the authorization entity. This protocol is intrinsically secure and effectively thwarts the man-in-the-middle attacks due to the fact that the communication between two ends is not in plain text. In practice, however, SSL may not be the protocol that is utilized between users and the authorization server. Regardless, the protocol used may utilize standard asymmetric cryptography through a key exchange in order to mitigate man-in-the-middle attacks.

2) SIMULATE THE USER's ENVIRONMENT

The proposed system utilizes what is in a user's environment to execute the second layer of authentication Figure 12. In this case, an identity thief scans the access points' information around the user, specifically the SSID, BSSID, and RSSI value of the access points. Then proceeds to replicate the environment somewhere else where they are in full control. First, from our point of view, the hacker has a low chance of gaining access due to a lack of availability of the user's credential information. However, if somehow an attacker was able to obtain the credential information, then the client's applications are necessary in order to gain access successfully to the system's server. A user's environment can still be sniffed, but attackers cannot make sense of them without the applications (the smartphone and desktop applications).

3) AN ATTACKER INSIDE A USER's ENVIRONMENT

Using a device that is Wi-Fi capable, the surrounding user's environment can be captured and furthermore, the RSSI values of the user's access points can be measured. In a case where an attacker was able to obtain the username and password of a user. While also being in the same place where the legitimate user is, Figure 13. In the proposed system, no one can communicate with the 0EISUA server without having the client-side's applications that are only available to legitimate users. Thus, the attacker might be able to collect the data in a user's environment but cannot even establish communication with the system's server without having the required applications.

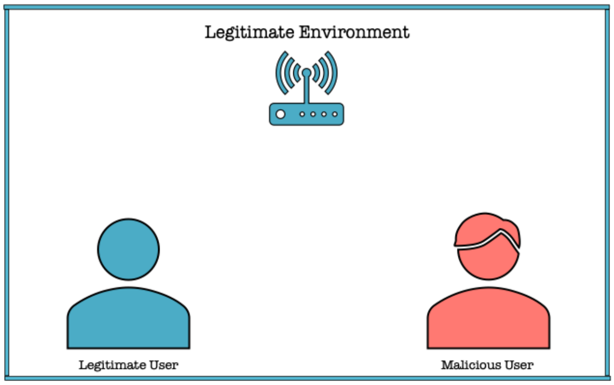


FIGURE 13. An attacker inside a user's environment.

C. USER CONVENIENCE

2FA mechanism enhances the security of a system. However, most of the time it comes at the expense of user convenience. In general, user convenience is a critical factor in determining how users make decisions about what to use.

The 0EISUA is a simplicity system in which when a user logs in with the benefits of 2FA, and without the normal hassle involved with significant user interaction (e.g., providing a pin, a phrase, a randomly generated code, or a physical key-based second factor). Since SFA methods are used as the standards for authentication (i.e., users almost always are expected to type in their username and password), our proposed method is as convenient as SFA, thus making its application readily usable and scalable.

Through the desktop and smartphone applications, the user communicates with the 0EISUA server. These applications are devolved to be suitable for any type of operating system (OS).

The internet is existent in almost all locations around the world and everywhere people can live [18]. Due to its nature of existing ubiquitously, the internet has recently become an essential and robust platform for education, business, and entertainment organizations. It is noted that locations with a reliable presence of internet connectivity are also places where access points are commonly established. Due to this factor, we consider our proposed system as a ubiquitous method since it relies on WiFi access points.

D. USABILITY

This research aims to add an extra layer of authentication by finding something unique in a user's environment – specifically, by utilizing information in ambient access points. Every access point broadcasts messages which carry distinctive information that can be used to identify a user's environment – and subsequently use the outcome to authenticate the user. In this paper, data within these broadcast messages are utilized to implement the second layer of authentication by determining if two devices are in the same physical location – and near enough to each other. In doing so, the proposed method can ensure that they belong to the same user. This system depends on something that a user knows, something that a user owns, and – a contribution of this work – something that is in the user's environment.

In the proposed system, both the login device and authentication device collect the broadcast beacon frames and measured the RSSI values from the access points then submit them to the 0EISUA server to authenticate a user. Furthermore, and quite importantly, this is done without any involvement from the users of the system.

The principal benefit of collecting embedded information from the beacon frames is that a wireless client can obtain and process the embedded information without necessarily being connected to the corresponding access points. Moreover, the beacon frames can be received only within a limited physical range of each wireless access point, thus limiting the potential for spoofing or impersonation (and arguably making the second factor more secure).

The proposed system can be used immediately without the requirements for additional hardware. Wi-Fi access points in the infrastructure can be utilized to achieve zero-effort two factors authentication. The proposed system does not require calibration and can use RSSI readings from the participating devices.

Implementing Zero Effort Indoor Secure User Authentication system in any organization provides many benefits. Including but not limited to, improving security, controlling access to a specific resource, reducing data theft, and decreasing the possibility of impersonating a user to gain access to a sensitive resource.

E. COST

The term Cost-effective means, a system is perfect and worthy comparing its benefits to its cost. The relationship between a system's cost and benefit could be a positive relationship where if one goes up the second follows or the opposite. In 0EISUA, what the user possesses (smartphone and desktop) and what is in the user's environment (WiFi access points) are employed, which will not cost extra money for utilizing it. Besides, no special hardware pieces are needed to be installed or used. This result in the system is not complex and easy to maintain.

In this section, the proposed system's security, cyber-attack vulnerability assessment, user convenience, and cost for an effective 0EISUA system were presented. Subsequently, we proposed a new 2FA system that requires no more than typing in a username and a password.

VI. CONCLUSION

As can be seen from the experiments, the proposed methodology results in a practical approach to authenticate a user based on the distance between the two devices if they are within a predefined acceptable range. Also, from the results, we believe that the proposed system is an efficient method to do so because its accuracy is quite acceptable at 93.3%, and there is no significant difference between an actual location and the calculated location. Note that the experiments were performed at a busy university, at different times of the day.

We believe that a zero-effort system will encourage the use of 2FA in more systems, primarily due to the convenience of SFA and the security of 2FA. Well, once the user has installed the application, 0EISUA requires no more intervention than simply entering the password as usual.

REFERENCES

[1] N. Karapanos, C. Marforio, C. Soriente, and S. Capkun, "Sound-proof: Usable two-factor authentication based on ambient sound," in *Proc. 24rd USENIX Secur. Symp. (USENIX Security)*, Washington, DC, USA: USENIX Association, 2015, pp. 483–498.

[2] K. Ahmad, M. Doja, N. Udzir, and M. Singh, *Emerging Security Algorithms and Techniques*. Boca Raton, FL, USA: CRC Press, 2019.

[3] X. Zhu, S. Yu, and Q. Pei, "QuickAuth: Two-factor quick authentication based on ambient sound," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

[4] D. Schürmann and S. Sigg, "Secure communication based on ambient audio," *IEEE Trans. Mobile Comput.*, vol. 12, no. 2, pp. 358–370, Feb. 2013.

[5] B. Shrestha, M. Shirvanian, P. Shrestha, and N. Saxena, "The sounds of the phones: Dangers of zero-effort second factor login based on ambient audio," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2016, pp. 908–919.

[6] M. Wang, W.-T. Zhu, S. Yan, and Q. Wang, "SoundAuth: Secure zero-effort two-factor authentication based on audio signals," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, May 2018, pp. 1–9.

[7] B. Shrestha, M. Shirvanian, P. Shrestha, and N. Saxena, "Sound-proof: Usable two-factor authentication based on ambient sound," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2016, pp. 483–498.

[8] M. H. Eldefrawy, K. Alghathbar, and M. K. Khan, "OTP-based two-factor authentication using mobile phones," in *Proc. 8th Int. Conf. Inf. Technol., New Generat.*, Apr. 2011, pp. 327–331.

[9] J. Yu and P. Brune, "No security by obscurity-why two factor authentication should be based on an open design," in *Proc. Int. Conf. Secur. Cryptogr.*, Jul. 2011, pp. 418–421.

[10] H. Fujii and Y. Tsuruoka, "SV-2FA: Two-factor user authentication with SMS and voiceprint challenge response," in *Proc. 8th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2013, pp. 283–287, doi: 10.1109/icitst.2013.6750207.

[11] B. Rodrigues, A. Chaudhari, and S. More, "Two factor verification using QR-code: A unique authentication system for Android smartphone users," in *Proc. 2nd Int. Conf. Contemp. Comput. Informat. (IC3I)*, Dec. 2016, pp. 457–462.

[12] A. Pratama and E. Prima, "2FMA-NetBank: A proposed two factor and mutual authentication scheme for efficient and secure Internet banking," in *Proc. 8th Int. Conf. Inf. Technol. Electr. Eng. (ICITEE)*, Oct. 2016, pp. 1–4.

[13] K. Reese, "Evaluating the usability of two-factor authentication," M.S. thesis, Dept. Comput. Sci., Brigham Young Univ., Provo, UT, USA, 2018.

[14] K. Krombholz, P. Fruhwirt, T. Rieder, I. Kapsalis, J. Ullrich, and E. Weippl, "QR code security–how secure and usable apps can protect users against malicious QR codes," in *Proc. 10th Int. Conf. Availability, Rel. Secur.*, Aug. 2015, pp. 230–237.

[15] W. A. Hufstetler, M. J. H. Ramos, and S. Wang, "NFC unlock: Secure two-factor computer authentication using NFC," in *Proc. IEEE 14th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Oct. 2017, pp. 507–510.

[16] D. Mahansaria and U. K. Roy, "Secure authentication for ATM transactions using NFC technology," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2019, pp. 1–5.

[17] V. Coskun, B. Ozdenizci, and K. Ok, "The survey on near field communication," *Sensors*, vol. 15, no. 6, pp. 13348–13405, 2015.

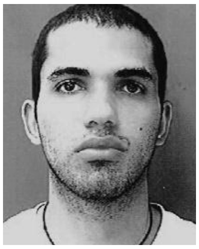
[18] X. Li and J. Li, *Quality-Based Content Delivery Over the Internet*. Shanghai, China: Shanghai Jiao Tong Univ. Press, 2011.

[19] L. J. Chu, "Physical limitations of Omni-directional antennas," *J. Appl. Phys.*, vol. 19, no. 12, pp. 1163–1175, Dec. 1948.

[20] *FCC Rules and Regulations 2.4 & 5 GHz Bands*, AIR802, Oswego, IL, USA, 2018.

ALI ABDULLAH S. ALQAHTANI (Student Member, IEEE) received the B.S. degree *(summa cum laude)* in computer science from Grambling State University, USA, in 2016, the M.S. degree in computer and information science with a concentration in cyber security and privacy from Southern Arkansas University, USA, in 2017, and the second M.S.Eng. degree in electrical engineering from Louisiana Tech University, USA, in 2018, where he is currently pursuing the Ph.D. degree in engineering-cyberspace engineering.

He has worked in fields of industrial, academia, research, and military, for more than 11 years. His primary area of research, in which he has participated, is designing multifactor authentication applications. He is also interested in security and privacy, with a focus on access control systems, and location-based services.



HOSAM ALAMLEH received the M.S. degree in electrical Engineering, in 2014, and the Ph.D. degree from Louisiana Tech University, Ruston, LA, USA, in 2019.

His employment experience included consulting and optimizing the radio frequency systems in different wireless communication companies in Jordan, UAE, and USA. Furthermore, he worked for a location technology company, in Mountain View, CA, USA.

JEAN GOURD (Member, IEEE) has worked on the development of security methods for mobile agents and performed extensive work on developing fundamental methods to model such agents within multiagent systems. He has an Active Research Program in the areas of cyber security, distributed systems, and software engineering. He is currently the Program Chair of computer science and an Associate Professor of computer science and cyber engineering with Louisiana Tech University. His research interests include cyber threat avoidance and cyber security education. He is also interested in cyber security methods that make threats simply not matter (i.e., avoiding them altogether) and ways to address the growing need for cyber security professionals. He is also involved in numerous ongoing research projects with the Air Force Research Lab (AFRL) and the Department of Defense (DoD), and maintains collaborative relationships with members of industry and national research laboratories.