RESEARCH ARTICLE

Leveraging Machine Learning for Wi-Fi-Based Environmental Continuous Two-Factor Authentication

ALI ABDULLAH S. ALQAHTANI[ID]**1, (Member, IEEE), THAMRAA ALSHAYEB**[ID]**2, MAHMOUD NABIL**[ID]**3, (Member, IEEE), AND AHMAD PATOOGHY**[ID]**1, (Senior Member, IEEE)**

[1]Department of Computer Systems Technology, North Carolina Agricultural and Technical State University, Greensboro, NC 27411, USA
[2]Department of Physics and Astronomy, George Mason University, Fairfax, VA 22030, USA
[3]Department of Electrical and Computer Engineering, North Carolina Agricultural and Technical State University, Greensboro, NC 27411, USA

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

ABSTRACT The traditional two-factor authentication (2FA) methods primarily rely on the user manually entering a code or token during the authentication process. This can be burdensome and time-consuming, particularly for users who must be authenticated frequently. To tackle this challenge, we present a novel 2FA approach replacing the user's input with decisions made by Machine Learning (ML) that continuously verifies the user's identity with zero effort. Our system exploits unique environmental features associated with the user, such as beacon frame characteristics and Received Signal Strength Indicator (RSSI) values from Wi-Fi Access Points (APs). These features are gathered and analyzed in real-time by our ML algorithm to ascertain the user's identity. For enhanced security, our system mandates that the user's two devices (i.e., a login device and a mobile device) be situated within a predetermined proximity before granting access. This precaution ensures that unauthorized users cannot access sensitive information or systems, even with the correct login credentials. Through experimentation, we have demonstrated our system's effectiveness in determining the location of the user's devices based on beacon frame characteristics and RSSI values, achieving an accuracy of 92.4%. Additionally, we conducted comprehensive security analysis experiments to evaluate the proposed 2FA system's resilience against various cyberattacks. Our findings indicate that the system exhibits robustness and reliability in the face of these threats. The scalability, flexibility, and adaptability of our system render it a promising option for organizations and users seeking a secure and convenient authentication system.

INDEX TERMS Two-factor authentication, machine learning, zero effort, continuous authentication, beacon frames, wireless access points, authentication module, Wi-Fi radio waves, RSSI values, 2FA, ML.

I. INTRODUCTION

As technology continues to advance at a rapid pace, the need for robust security measures to safeguard sensitive information and data has become paramount. The Identity Theft Resource Center (ITRC) report reveals that data breaches have surged by over 68% in 2020, with a total of 1,862 incidents [1]. In response to these threats, the adoption of Two-Factor Authentication (2FA) has seen a significant

The associate editor coordinating the review of this manuscript and approving it for publication was Rongbo Zhu[ID].

growth. Google's 2020 study indicates that 150 million people employ 2FA to secure their accounts, the number is expected to rise as cybersecurity takes precedence among individuals and organizations [2]. Microsoft's research corroborates the effectiveness of 2FA, demonstrating that it can thwart 99.9% of automated cyberattacks [3]. As a result, 2FA has become an indispensable tool for protecting sensitive data. A survey by the Ponemon Institute further underscores its importance, showing that 56% of U.S. organizations have implemented 2FA for at least a portion of their workforce [4].

As 2FA necessitates two authentication factors from users to augment the security beyond a mere password, the adoption of the second factor has become a research question and investigated in [5], [6], and [7]. Researchers have used a range of factors encompassing knowledge-based, possession-based, inherence-based, location-based, behavioral-based, and ambient-based factors [8]. Each approach aims to uniquely verify a user's identity while bolstering information security.

However, existing 2FA techniques possess limitations, including user inconvenience, susceptibility to human error, single-point authentication, restricted adaptability, scalability challenges, and inflexibility. To tackle these issues, this paper introduces a novel 2FA system that harnesses Wi-Fi radio waves and Machine Learning (ML) to authenticate a user's identity. The proposed system strives to deliver a seamless, user-friendly 2FA experience that minimizes the need for users to supply additional authentication factors beyond their primary login credentials. Furthermore, the proposed system addresses the limitations of existing 2FA methods, enhancing scalability, adaptability, and flexibility.

This paper is an extension of our previously published paper [9]. The new contributions with respect to the older version are listed below:

- We have incorporated four more ML models to develop an ML-based 2FA system that leverages Wi-Fi access point broadcast messages and RSSI values for reliable and secure user authentication. These models help eliminate the need for additional user input or action, reducing human error risks and improving the overall user experience.
- We have incorporated continuous authentication into our system, which enhances security by constantly verifying the user's identity while accessing protected resources, effectively thwarting unauthorized access.
- We conducted a Feature Importance analysis, which provides insights into the significance of each feature in the classifications made by the ML models in the proposed system.
- We evaluated the computation overhead of the proposed system in implementing the second layer of authentication using different ML models.
- We have conducted a comprehensive security analysis of our proposed system to evaluate its resilience against potential cyberattacks, including evasion attacks, model extraction attacks, and radio frequency signal interference attacks.

The remainder of this paper structure is organized as follows: Section II discusses ML-based secure authentication and continuous 0E2FA methods for various applications. Section III presents a detailed description of the network and threat models for the proposed system. In Section IV, we present the proposed system and how it uses beacon frames and RSSI values to verify a user's identity. Section V describes the experiments conducted to evaluate the proposed system, including the dataset used, the performance metrics calculated, and the results obtained. In section VI, we discuss the security analysis of the proposed 2FA system by examining its vulnerability to various cyberattacks and evaluating its resilience against them. Section VII discusses the proposed system's features, including reliability, zero-effort authentication, continuous authentication, adjustability, scalability, flexibility, and a one-time login solution. Section VIII concludes and summarizes the key points and contributions of the proposed system.

II. RELATED WORK

Various secure authentication mechanisms utilizing ML have been proposed for different applications [10], [11], [12], [13], [14]. For instance, Gupta et al. [15] proposed a secure authentication mechanism that uses ML and nonce-based systems for a telecare medical information system. Punithavathi et al. [16] introduced a cloud-based cancelable biometric authentication system for IoT devices. In [17], the authors propose a deep-learning-based active authentication method that utilizes sensors in consumer-grade smartphones to authenticate users. Furthermore, a mouse data protection technology is introduced in [18] that generates random mouse positions to protect mouse data and uses ML to verify its security. A novel technique for secure access to smartphones utilizing piezoelectric touch sensing supported keystroke dynamics to authenticate users was proposed [19]. An IoT authentication system based on ML that uses human impedance as a user identifier is also introduced in [20]. Furthermore, the integration of ML techniques into a DevOps ecosystem to develop a Risk Authentication/Assessment Decision Engine (RADE) that estimates the risk level of each authentication attempt is presented in paper [21]. Lastly, a new two-factor authentication scheme based on real-time keystroke dynamics using the K-nearest neighbor classification algorithm is introduced in [22].

In the field of secure communication, two recent papers propose novel methods for authentication using physical layer features and deep learning algorithms. The first paper presents a framework for preventing spoofing attacks in Controller Area Networks (CANs) by exploiting physical layer features and using reinforcement learning to choose the authentication mode and parameter [23]. The proposed scheme employs a deep learning approach to further enhance authentication efficiency.

In [24], Oligeri et al. investigate the use of AI-based solutions for physical-layer authentication of Low-Earth Orbit (LEO) satellites, a challenging scenario due to non-standard electronics and unique attenuation and fading characteristics. The study uses Convolutional Neural Networks (CNN) and autoencoders to authenticate satellite transducers with high accuracy but highlights the potential limitations due to the high number of I-Q samples required and the low bandwidth of satellite links.

Various Zero-Effort Two-Factor Authentication (0E2FA) mechanisms that aim to authenticate users without requiring

extra user interaction were published [25], [26], [27], [28], [29]. The paper, [30], leverages environmental Bluetooth Low Energy (BLE) signal characteristics for co-location detection, while SoundAuth [31] uses ambient audio signals and ML techniques for authentication. The proposed system in [32] captures gait patterns using a smartphone and smart-watch/bracelet, and Vibe [33] uses vibration communication for user authentication.

Another study [34] presents a smart hotel access system that uses Near Field Communication (NFC) Host-Card Emulation application for authentication. These mechanisms provide more secure and reliable solutions for zero-effort authentication while maintaining user-friendliness. They have been tested and evaluated for usability and security, and they demonstrate good resistance to attacks and high detection accuracy. The vulnerability of touch-based continuous authentication systems (TCAS) to active adversarial attacks is investigated in [35].

The significant role of security incidents caused by insiders in attacks against organizations is addressed in [36], which proposes a continuous authentication solution for large multi-site enterprises based on Apache Spark, Apache Cassandra, Kafka, and a MySQL database.

A novel authentication mechanism for smartphones that utilizes gait patterns and keystroke dynamics as behavioral biometrics to establish a multimodal biometrics profile is proposed in [37]. The experimental results demonstrate the robustness and security of the proposed method against different types of attacks.

Finally, a behavioral biometrics approach for exoskeletons using wearable sensors to ensure the user's identity and authority during operation is proposed in [38], which could be useful for other wearables used in robot control.

Recent advancements in adversarial attack methodologies proposed for DL-based wireless signal classifiers aimed at anti-eavesdropping have been highlighted in [39]. In contrast, our research primarily centers on developing two-factor authentication. By utilizing ML for continuous identity verification based on environmental features, we emphasize providing secure and convenient user authentication without directly addressing adversarial attack techniques.

III. NETWORK & THREAT MODELS
This section provides a detailed description of the network model used in the proposed 2FA system, as well as explores the threat model of the system.

A. NETWORK MODEL
In the proposed 2FA system, at least one Wi-Fi Access Point (AP) must be present in the user's environment. This AP will transmit beacon frames containing unique characteristics. For system use, the user needs two Wi-Fi-enabled devices (e.g., a smartphone and a laptop). The laptop/PC acts as a login device, and the smartphone serves as a mobile device. Both devices must contain applications that collect and transmit
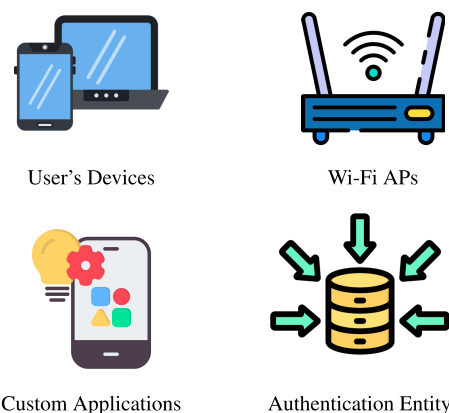

FIGURE 1. Required components; icons from [40].

data to the authentication entity. Below is a list of the required components, see Figure 1:

1) Device Requirements: the proposed system necessitates the utilization of two distinct devices for authentication purposes: a login device and a mobile device. The login device, such as a computer, allows the user to access the system, while the mobile device, typically a smartphone, is carried by the user to send and receive beacon frames.

2) APs: The system relies on APs to disseminate beacon frames for user authentication. These APs can be any wireless AP compatible with IEEE 802.11 standards, including Wi-Fi APs.

3) Custom Applications: To facilitate the authentication process, our system mandates the use of specialized applications on both the login and mobile devices. These applications are responsible for the transmission and reception of beacon frames and for communication with the server and database.

4) Authentication Entity: This component is in charge of storing user authentication data and orchestrating the authentication procedure. By receiving and processing beacon frames and RSSI values from user devices (i.e., a login device and a mobile device), it makes informed authentication decisions based on the properties of these frames. The authentication entity consists of the following sub-components.

a) A database that stores the selected beacon frame characteristics i.e., SSID, BSSID (i.e., uses only in step 4 in Figure 2), and Wi-Fi radio waves frequency) and RSSI values collected from the user's devices, as well as the user's login credentials and other necessary information required for the authentication process. In general, Wi-Fi beacon frames contain various characteristics that serve specific purposes in network operations. However, not all of these characteristics have a direct impact on device localization. By focusing on the ones that directly affect device localization (i.e., SSID, BSSID, Wi-Fi radio wave frequency) and RSSI - we can streamline the localization process, reduce

computational complexity, and develop an effective solution for real-world applications.

b) An authentication module that utilizes an ML algorithm analyzes the collected data from the user's devices and makes the final decision on whether to grant the user access to the authentication entity.

During the registration phase, the users must activate and create their account through the custom mobile application. Once logged in, the application runs in the background, waiting for instructions from the authentication entity. Every time the user wants to use the system, the application automatically scans their environment and transmits the collected data to the authentication entity. The process is seamless and does not require the user to take any additional actions through the mobile application.

B. THREAT MODEL

The proposed system considers two primary categories of potential attackers: internal and external. Individuals who possess authorized access to the system, such as employees, contractors, or those with insider knowledge of the system's architecture, algorithms, and data, fall under the internal attackers category. Such attackers may exploit their access or knowledge to compromise the system's security from within by manipulating input data or ML models to achieve their objectives.

External attackers, on the other hand, are individuals or entities without authorized access to the system. These attackers typically exploit vulnerabilities in the system from outside by intercepting communications, finding weaknesses in the algorithms, or compromising the infrastructure that supports the system.

The proposed 2FA system, relying on radio waves and ML, is susceptible to a range of security threats that can undermine its performance and security. Attackers can exploit weaknesses in the ML models, manipulate input data, or obstruct communication channels, leading to the system's compromise. The considered threats in this work include *evasion*, wherein malicious inputs are created to bypass the detection mechanisms, *model extraction*, which involves reverse-engineering the ML model to gain unauthorized access, and radio frequency signal interference attacks that disrupt the communication channels by emitting conflicting signals, reducing the system's ability to operate effectively. These threats are discussed and examined in Section VI.

IV. THE PROPOSED SYSTEM

This section provides a detailed description of the proposed system. Specifically, we will discuss the authentication process and the features of the proposed system. Before utilizing the system, users must create a profile and download the required applications; discussed early in Subsection III-A.

A. AUTHENTICATION PHASE

The proposed authentication follows a multi-layered approach to access protected entities. The first layer
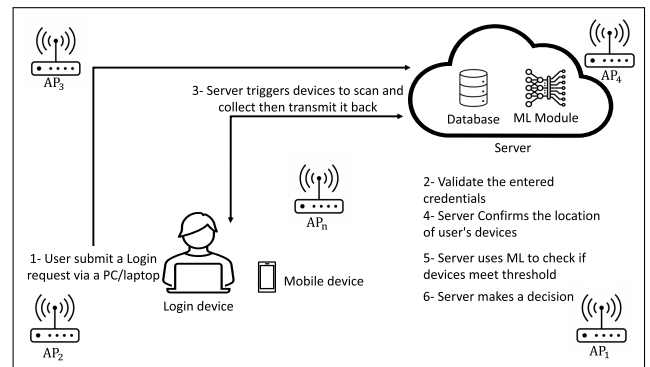

FIGURE 2. System configuration & authentication process.

requires users to enter a valid username and password for authentication. After this, the second authentication layer requires users to satisfy two criteria. The first criterion mandates that both the user's devices (i.e., a login device and a mobile device) are present in a predefined number of overlapped Wi-Fi access points that are visible to both devices. The second criterion demands that the devices are within a specific proximity threshold; more details will be presented in Subsection IV-B3.

We assume that the determination of the number of overlapping Wi-Fi APs and the proximity threshold is conducted through an administrative process that considers the particular security needs of the protected entity.

The proposed authentication process aims to balance convenience and security by minimizing the user's burden while ensuring reliable authentication. To provide readers with a clearer understanding of the system configuration and underlying processes, we further detail our algorithm and models. The subsequent sections will delve into the specifics. Figure 2 illustrates the system configuration and steps involved in the process:

1) The user attempts to access the authentication entity and enters his/her login credentials (username and password).

2) The server validates the credentials by checking them against the stored user profile.

3) The server triggers the user's devices (i.e., a login device and a mobile device) to collect the selected beacon frame characteristics and measure RSSI values from the Wi-Fi APs in the user's environment, and transmit them to the server.

4) In order to confirm the location of the user's devices, the server checks that both devices can detect a predefined number of overlapping Wi-Fi APs. This is done by comparing the unique identifiers (SSIDs and BSSIDs) of the Wi-Fi APs. Both devices will scan and detect Wi-Fi APs in his/her vicinity and create a list of the Wi-Fi APs that have matching SSIDs and BSSIDs. By identifying overlapping Wi-Fi APs, the server can confirm that the user's devices are in close proximity to one another.

5) The server uses ML to analyze the collected data from the user's devices (i.e., a login device and a mobile device) to determine if the devices are within the predefined threshold or not.
6) The final decision is made based on the joint success of steps 4 and 5. If both are successful, access is granted; if not, access is denied.

It is essential to note that while our authentication may seem to follow a binary decision framework (access granted or denied), the underlying processes involve intricate analyses. The binary classification approach was chosen for its suitability in authentication scenarios. Here, a user is either authenticated or not, making it inherently binary. However, the complexity arises in making this binary decision, which involves multi-layered checks, continuous monitoring, and ML-based evaluations. These intricacies go beyond mere binary results and are pivotal for ensuring robust and reliable authentication.

B. THE PROPOSED SYSTEM FEATURES

In this subsection, we will explain the features of our system incentives. Then, we will compare these features against the discussed related works in Subsection IV-C.

1) ZERO-EFFORT

The proposed system has a ''zero-effort'' feature or ''Noninteractive'', which significantly enhances the user experience by automating the authentication process, eliminating the need for additional input or action. By employing ML to analyze the selected beacon frame characteristics and RSSI values from users' devices (i.e., a login device and a mobile device) the system efficiently implements the second layer of authentication and verifies their identity; steps 4 and 5. This seamless approach not only boosts user satisfaction but also bolsters security through the reduction of human error risks, ultimately resulting in a streamlined and secure authentication experience.

2) CONTINUOUS AUTHENTICATION

The continuous authentication feature in the proposed system enhances security by constantly verifying a user's identity while they access protected resources; repeating step 5 in Figure 2. Utilizing ML technology, the system analyzes distinctive environmental characteristics and signals to ensure that the user's devices remain co-located. If the devices are no longer in the same location, the session is promptly terminated. This approach not only improves security by thwarting unauthorized access but also offers user convenience and alleviates the need to remember to log out, resulting in a seamless and secure experience; this feature will be examined in the experiment presented in Section V-D and achieved a 100% success rate in terminating the session when the user's devices were not co-located.

TABLE 1. Comparison with the discussed works, where ✓: Feature Supported, and ✗: Not supported.

Study	Noninteractive	Continuum	Adjustability	Flexibility
[10]–[24]	✗	✗	✗	✗
[25]–[38]	✓	✓	✗	✗
Ours	✓	✓	✓	✓

3) ADJUSTABILITY

The adjustability of the proposed system plays a crucial role in providing a high level of security, as it facilitates the customization of the access policy process according to the distinct needs of each protected entity. By modifying key factors, such as the number of Wi-Fi APs involved in users' identity verification and the distance threshold (i.e., used in the authentication process, steps number 4 and 5 in Figure 2), the system can be fine-tuned to address the security requirements of a wide range of systems and data types. This adaptability enables a tailored security solution that effectively accommodates varying levels of protection, ensuring that each entity's unique demands are met without compromising the overall performance and reliability of the system.

4) FLEXIBILITY

The proposed system's use of broadcast messages is a crucial element of its flexibility. By relying on broadcast messages (i.e., used in the authentication process, step number 3), the system can easily adapt to different settings without significant modifications. This allows the system to be deployed in various environments without requiring extensive customization, reducing the time and cost associated with implementation. The use of ML further enhances the system's flexibility by enabling it to adjust to the unique characteristics of each user's environment. This means that the system can accurately identify users, regardless of their location or device. As a result, the proposed system is a highly versatile solution that can be applied to a wide range of environments, providing an adaptable and robust security solution.

C. COMPARISON WITH THE DISCUSSED RELATED WORKS

Although several 2FA methods have been proposed and disucsieed in Section II, we believe that the community needs to put some efforts to progress the field. Reviewing the related works show that almost each and every of the proposed methods suffer from at least one of the desired criteria for 2FA e.g., interactability, continuum, adjustability, and flexibility. Table 1 summarizes this claim and compares our proposed method against methods of the literature. Later on, we will discuss how each of these criterion is supported in our method in their respective subsections.

V. EXPERIMENT

In this section, we describe the experimental setup utilized to evaluate the proposed authentication system.

A. SYSTEM CONFIGURATION

The system configuration consisted of the following components.

1) Wi-Fi APs: A total of ten APs were detected by the system utilizing publicly available Wi-Fi APs in a North Carolina A&T research laboratory on a typical school day to simulate a busy building setting. It is noteworthy that the detection of radio waves from the APs did not require any connection to them.

2) User devices: Raspberry Pi 3 Model B boards were employed to mimic the users' two devices, namely, the mobile device and the login device.

3) Server: A desktop computer with Ubuntu 16.04 LTS (64-bit) as the operating system was utilized to run the computer and host the ML module. Additionally, PhPmyadmin was used to create and execute the database.

B. DATA COLLOCATION PHASE

The purpose of the data collocation phase was to gather sufficient data to train the proposed system's ML module to determine the location of the user's devices based on the chosen beacon frame characteristics and RSSI values from Wi-Fi APs. To collect the data, a maximum threshold distance of 7 feet between the user's devices was established.

Two datasets were then collected: an *"authentic"* dataset with data collected when the two Raspberry Pis were within 7 feet of each other, and an *"unauthorized"* dataset with data collected when the distance between the Pis was greater than 7 feet (a minimum distance of 7.5 feet). To diversify the data samples, the Pis were repeatedly placed at varying distances for both datasets.

This approach helped identify the *"gray area"* between the acceptable threshold distance and the distance at which access should be denied. A total of 4,825 data samples were collected from two Raspberry Pis for the two datasets, with 2,442 samples in the *"authentic"* dataset and 2,383 samples in the *"unauthorized"* dataset. This near-equal distribution helps in preventing biases in the ML model towards either category. These samples were collected from 10 different Wi-Fi access points located in various positions within the experimental areas and at different times.

The resulting datasets consisted of six columns: "RPi", "SSID,", "Frequency (Hz)", "RSSI (dBm)", "Location", and "Label." In our datasets, the independent variables include "RPi" (which Raspberry Pi collected the data), "SSID" (name of the Wi-Fi AP), "Frequency (Hz)" (frequency of the Wi-Fi AP), and "RSSI (dBm)" (RSSI value in dBm). These variables represent the factors that we manipulated or observed to see their effect on the dependent variable. The dependent variable in our study is "Label," a binary variable indicating whether the sample is "authentic" (1) or "unauthorized" (0). This dependent variable reflects the outcome we are interested in predicting based on the independent variables.

FIGURE 3. Dataset visualization.

TABLE 2. Evaluation results.

Model	Accuracy	Sensitivity	Specificity	F1 Score	Precision
DT	0.924	0.918	0.932	0.926	0.934
KNN	0.923	0.911	0.936	0.924	0.938
RF	0.922	0.92	0.925	0.924	0.929
SVM	0.903	0.895	0.91	0.904	0.914
NB	0.885	0.849	0.923	0.884	0.921
LR	0.881	0.891	0.87	0.885	0.879

The datasets were curated to ensure a balance between the "authentic" and "unauthorized" samples.

For empirical evaluation, we employed the N-fold cross-validation technique. Specifically, we utilized 5-fold cross-validation in our analysis. This involved dividing the dataset into five parts, using four parts for training and one part for testing iteratively.

In the evaluation phase, we partitioned our labeled data into a training set (80%) and a testing set (20%). Six different ML models were employed to evaluate the proposed system, namely Decision Tree (DT), K-Nearest Neighbors (K-NN), Random Forest (RF), Support Vector Machine (SVM), Naive Bayes (NB), and Logistic Regression (LR). The selection of these models was based on their effectiveness in similar classification tasks. We computed the confusion matrix for each model and used the five standard evaluation metrics for classification tasks in ML: accuracy, sensitivity, specificity, F1 Score, and precision. The confusion matrices for the DT, KNN, RF, SVM, NB, and LR models are presented in Figure 4.

As can be seen from Table 2, the DT and KNN models perform the best overall, with DT achieving the highest accuracy and F1 Score, and KNN obtaining the highest specificity and precision. RF also performs well with the highest sensitivity.

C. FEATURE IMPORTANCE

The Feature Importance analysis was conducted to understand the significance of each feature in the classifications made by the ML models within the proposed system. This information is instrumental in identifying the key features that drive the model's accuracy. We determined the feature importance for DT, RF, KNN, SVM, and LR. However, this metric is not applicable to the NB model. Since NB is a probabilistic model, it assumes conditional independence among features given the target class and does not account for feature interactions or correlations when classifying.

Identifying feature importance enables us to pinpoint the most crucial factors in generating accurate predictions. In our Python implementation, we used the *feature_importances_* attribute to directly obtain the importance of each feature for DT and RF models. For KNN,

Decision Tree Confusion Matrix

K-nearest Neighbors Confusion Matrix

Random Forest Confusion Matrix

Support Vector Machine Confusion Matrix

Naive Bayes Confusion Matrix

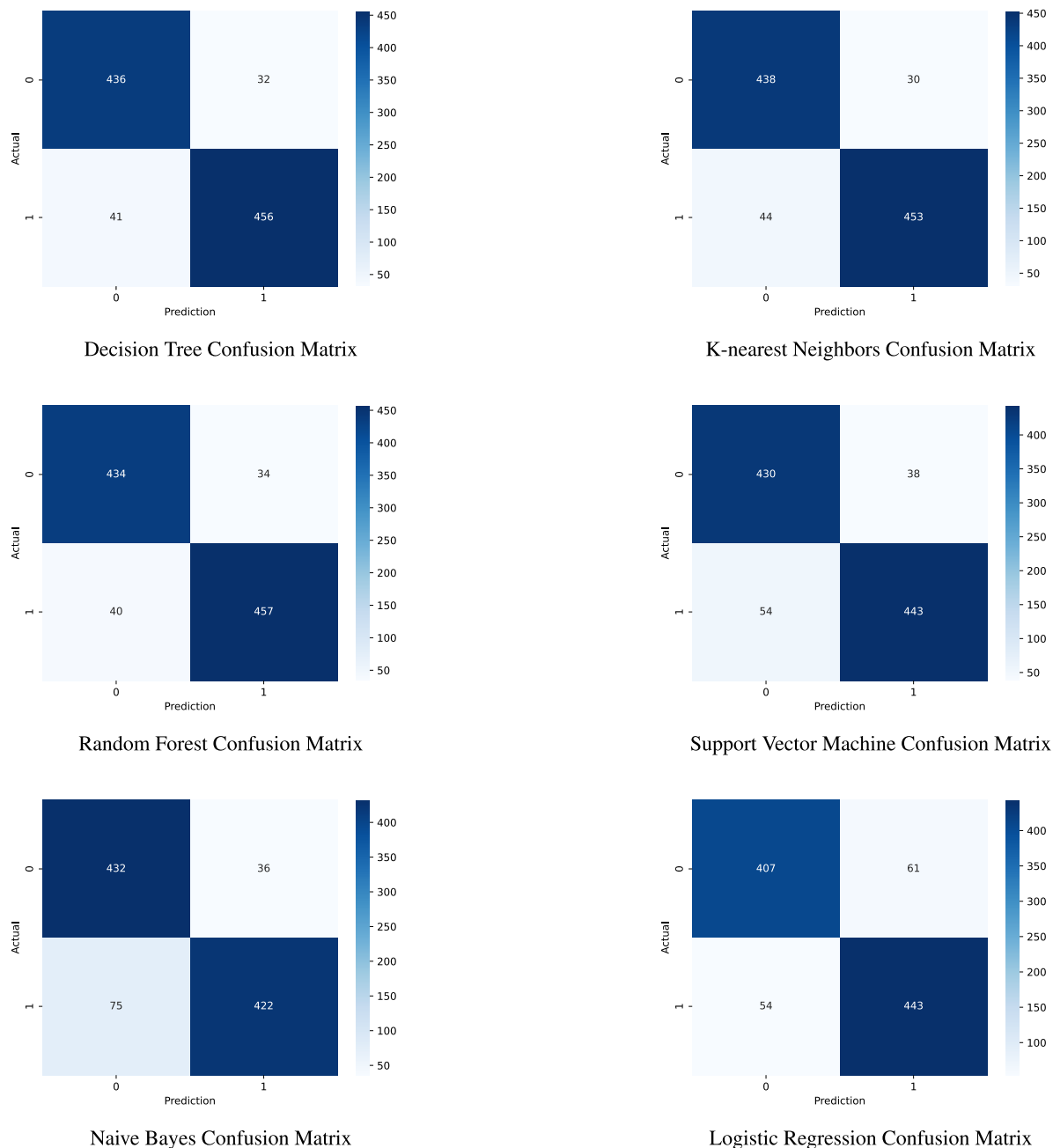Logistic Regression Confusion Matrix

FIGURE 4. Confusion matrices for various classifiers.

we employed the *mutual_info_classif* function from the *sklearn.feature_selection* module to compute the mutual information between each feature and the target variable. Lastly, we determined feature importance for SVM and LR models by utilizing the absolute value of the coefficients, accessed through the *coef _* attribute.

Table 3 presents our results. In the DT model, the most important feature is RSSI (dBm), with a 70.79% score, followed by Frequency (Hz) at 17.42%. For the KNN model, RSSI (dBm) remains the most crucial feature, contributing

TABLE 3. Feature importance results.

Model	RPi	SSID	Frequency (Hz)	RSSI (dBm)	Location
DT	0.18%	7.82%	17.42%	70.79%	3.79%
KNN	0.34%	0.18%	19.75%	30.10%	4.80%
RF	1.13%	7.28%	27.70%	54.56%	9.32%
SVM	0.01%	65.20%	13.04%	21.75%	0.01%
LR	0.61%	55.20%	1.19%	37.09%	5.91%

30.10%, while Frequency (Hz) accounts for 19.75%. In the RF model, RSSI (dBm) again holds the highest importance at 54.56%, with Frequency (Hz) coming in second at 27.70%.
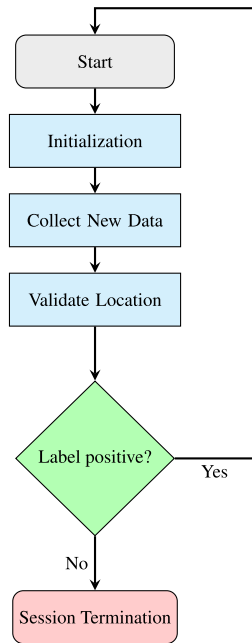
FIGURE 5. Continuous authentication Fluxogram.

Intriguingly, the SVM model identifies SSID as the most important feature with a 65.20% score, and RSSI (dBm) follows at 21.75%.

From Table 3, it is evident that RSSI (dBm) is the most significant feature for DT, KNN, and RF models, while the SVM and LR model prioritizes SSID. Other features, such as RPi, Frequency (Hz), and Location, exhibit varying levels of importance across different models.

D. CONTINUOUS AUTHENTICATION

To simulate continuous authentication using the proposed system, an algorithm was developed and translated to Python code that both mimics the system and continuously monitors the user's environment. The continuous authentication process, outlined in Figure 5, involves monitoring the location of the user's devices (i.e., a login device and a mobile device) and terminating the session if they are no longer in the same location.

The continuous authentication feature collects new Wi-Fi characteristics data from the user's APs using a loop, with each iteration processing the collected data using previously trained ML models, including DT, KNN, RF, SVM, NB, and LR. The loop identifies the label for the new data using each model in the list. If any of the models classifies a negative label, indicating that the user's devices (i.e., a login device and a mobile device) are no longer co-located, the session terminates, and the loop exits. If the label is positive, the loop waits for a specified interval of 30 seconds, which is most commonly supported by devices for scanning at intervals of 30 seconds or longer, before conducting another check.

This process repeats continuously until the session is terminated by a negative label classification or a user ends the session. In the experiment, the system was tested by

TABLE 4. Time consumption.

Model	DT	KNN	RF	SVM	NB	LR
Time	0.002 s	0.009 s	0.1 s	0.263 s	0.001 s	0.007 s

TABLE 5. Quantitative comparison with the discussed works, where NM: Not Mentioned.

Study	Number of Factor	Accuracy	Time Consumption
[10]–[24]	1-2	87% - 98.5%	NM
[25]–[38]	1-2	90% - 99.11%	NM
Ours	3	92.4%	0.001s - 0.263s

increasing the distance between two Raspberry Pis beyond the threshold of 7 feet after access was granted. Once the proposed system detected that the user's devices (i.e., a login device and a mobile device) were no longer in range (after the predetermined interval of 30 seconds), the session terminated immediately. Ten trials were conducted, and the proposed system achieved a 100% success rate in terminating the session when the user's devices were not co-located.

E. COMPUTATION OVERHEAD

The presented experiment measures the time required for the proposed authentication system to make decisions using six different ML models: DT, KNN, RF, SVM, NB, and LR. The processing time for each ML model is reported in seconds in Table 4.

Based on the results, the proposed authentication system demonstrates efficiency in implementing the second layer of authentication, with the maximum time taken by any ML model being 0.263 s, indicating satisfactory overhead for the processing time.

F. QUANTITATIVE COMPARISON WITH THE DISCUSSED RELATED WORKS

The quantitative comparative analysis presented in Table 5 underscores a notable trend in the extant literature: a predominant focus on accuracy, often at the expense of addressing efficiency. While many studies have achieved commendable accuracy rates, the conspicuous absence of efficiency metrics suggests a potential oversight in holistic model evaluation.

Our research endeavors to bridge this gap. By not only achieving a competitive accuracy rate of 92.4% but also emphasizing the model's efficiency, clocking in between 0.001s to 0.263s, we present a more comprehensive evaluation framework. This balanced approach underscores our model's applicability in diverse real-world scenarios, catering to both the need for correct classifications and timely outputs. Such a dual-focused evaluation approach is pivotal in advancing the field, ensuring that future models are not only accurate but also pragmatically efficient.

One of the standout features of our research is the deployment of a three-factor authentication system, highlighted in the "Number of Factor" column. While many conventional methods lean on 1-2 factors, typically passwords or biometrics, our approach presents a distinctive triad.

First, there is the Explicit Authentication, where users are prompted to input a valid username and password. Following that, we introduce two continuous, non-interactive, or "zero-effort" phases: Proximity and Device Presence and Zero-Effort Authentication. In the former, authentication is contingent upon both user devices (i.e., a login device and a mobile device) being present within overlapping Wi-Fi access points and staying within a designated proximity threshold. The latter employs ML to effortlessly authenticate users based on beacon frame characteristics and RSSI values from their devices, without requiring any further interaction from them.

VI. SECURITY ANALYSIS

In this section, we examine the security of the proposed 2FA system and assess its resilience against various cyberattacks.

A. EVASION ATTACKS

In the context of the proposed 2FA system, an evasion attack could occur if an attacker attempts to manipulate the RSSI values to deceive the system. Continuous authentication is a key feature of the proposed system that can mitigate evasion attacks. By continuously monitoring the user's environment, the system can detect anomalies in the RSSI values that may indicate an attack attempt. The system can then take appropriate actions, such as requesting additional authentication from the user, or even blocking access to the account.

To evaluate the system's resilience against such attacks, we assess the system's performance when an attacker manipulates the RSSI values to deceive the system. We simulate an evasion attack by adding random noise to the RSSI feature of the test data and evaluating the system's performance on the modified test data. To this end, we fit each ML model to the training data and then test the system's performance on the noisy test data, see Figure 6. As shown in Figure 9a, the system's performance remains relatively stable for most of the classifiers even when random noise is added to the RSSI feature of the test data, indicating that the system is not significantly affected by an attack attempt. This result suggests that the proposed system is robust against evasion attacks.

B. MODEL EXTRACTION ATTACK

Model Extraction attack involves an adversary attempting to extract the parameters or structure of a ML model by training a separate "shadow model" based on the outputs of the original model. Once the shadow model is trained, the adversary can use it to make predictions about new data and compare these predictions to the outputs of the original model to learn more about the structure and parameters of the original model. To mitigate the Model Extraction attack, we use model ensembling, which involves training multiple models on the same dataset and combining their outputs to make a prediction. This makes it more challenging for attackers to extract the parameters of any single model, since
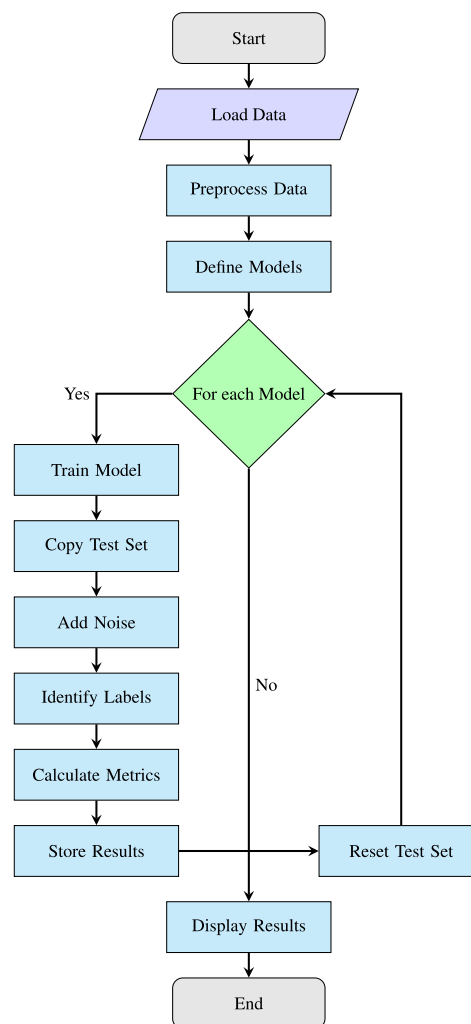

FIGURE 6. Evasion attack simulation Fluxogram.

they would need to extract the parameters of all of the models to gain a complete understanding of the system.

We loaded a dataset and trained a RandomForest (RF) model on it. To simulate a Model Extraction attack, we created adversarial examples by significantly altering the RSSI (dBm) values in the dataset. Using these adversarial examples and the predictions from our original RF model, we trained a shadow RF model. We then evaluated the shadow model's performance on the original test data to gauge its ability to approximate the original RF model's behavior. This entire process is detailed in Figure 7.

Figure 9b shows the performance of the attack model, indicating that the targeted model (RF) was affected by this type of attack, while the rest were not affected. These results demonstrate the effectiveness of our proposed system's model ensembling approach in mitigating the Model Extraction attack.

C. RADIO FREQUENCY SIGNAL INTERFERENCE ATTACK

Radio Frequency Signal Interference Attack is a cyberattack that disrupts wireless communication between two devices
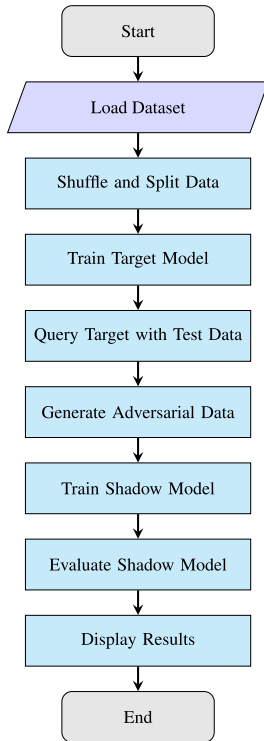
FIGURE 7. Model extraction attack simulation Fluxogram.

FIGURE 8. Radio frequency signal interference attack simulation Fluxogram.

(i.e., a login device and a mobile device) by transmitting radio signals. The attacker injects unauthorized radio signals into the wireless network, causing signal degradation, packet loss, and potentially unauthorized access to sensitive information. Continuous authentication can also help mitigate the effects of this attack by constantly monitoring the user's environment and comparing it with the data collected during the initial login. If there is a significant deviation from the original data, the system can assume that an attack is underway and either deny access or request additional authentication measures.

We simulated RF signal interference attack by adding random noise to the feature data using NumPy's *'random.normal()'* function; see Figure 8. The Interference variable is generated using this function with a normal distribution having a mean of zero and a standard deviation of 2. The noise is added to the feature data *'x'* by adding Interference to it, creating a new array *'x_noisy'*.

The results of our experiment indicate that the proposed system demonstrated a high level of resilience to this type of attack, even when subjected to significant interference. Figure 9c provides a visual representation of the results obtained.

VII. SYSTEM ANALYSIS

In this section, we discuss the proposed system features, each one in its own subsection.

A. RELIABILITY

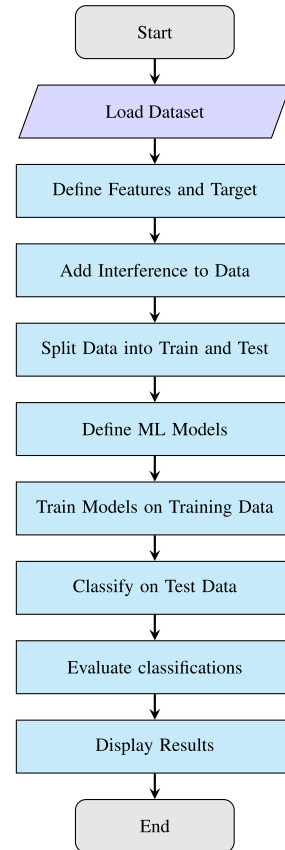ML is employed in our authentication system to bolster reliability and precision, circumventing the limitations of traditional two-factor methods that often necessitate manual input of codes or tokens. By analyzing the user's environment, ML eradicates the need for user input and mitigates human errors, thereby enhancing the system's dependability. The self-adaptive capability of ML minimizes the necessity for frequent maintenance or updates, rendering the system cost-efficient.

Our proposed scheme demonstrates outstanding reliability, as evidenced by a 92.4% success rate in implementing the second layer of authentication in our experimental results, as presented in Table 2. Before implementing the second layer of authentication, the system must achieve a 100% success rate in authentication steps number 1, 2, and 4 in Figure 2. We further evaluated its robustness under adversarial conditions by introducing various attack scenarios in Section VI. Even in these challenging circumstances, the highest time for a successful login using ML remained at a swift 0.263 seconds as can be seen from Table 4. Collectively, these factors contribute to the system's robust performance, instilling confidence in its practical, real-world applications.
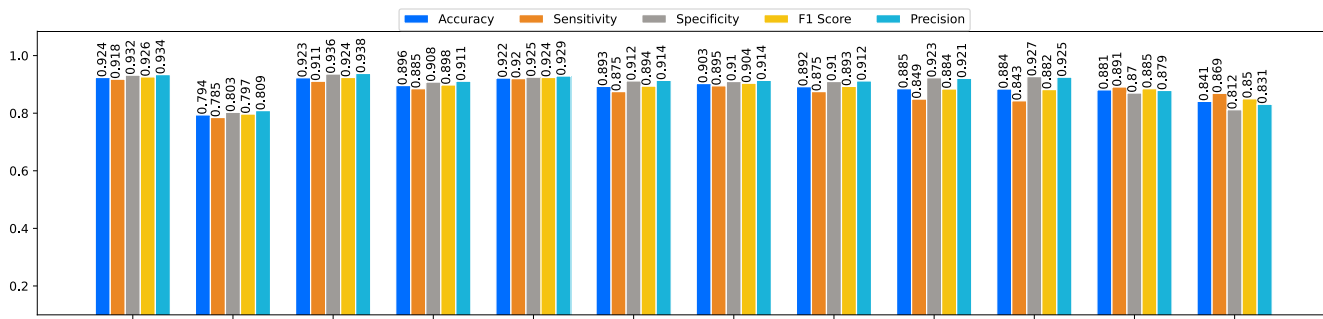
B. SCALABILITY

The proposed system that utilizes broadcast messages from Wi-Fi APs to authenticate users relies heavily on the scalability of the system to handle an increasing number of users and devices smoothly. Smart devices, like mobile
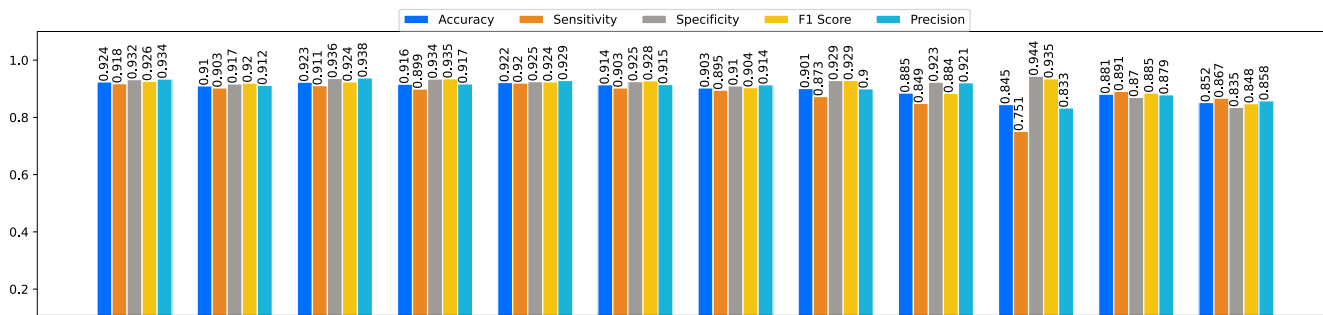
(a) Simulate Evasion Attack Result Visualization
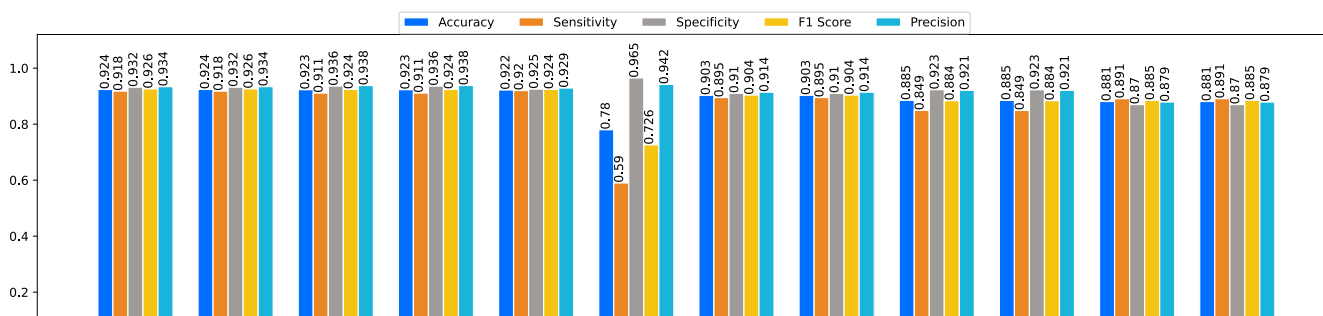
(b) Simulate Model Extraction Attack Result Visualization

(c) Simulate RF Signal Interference Attack Result Visualization

FIGURE 9. Combined attack result visualizations; Modal's name with apostrophe indicates result after attack.

phones, laptops, and tablets, can detect signals from various radio frequency sources in their vicinity, and as they move between networks, they receive broadcast messages from APs containing useful information.

This allows for high scalability, as any Wi-Fi-enabled device within range can receive and process the messages, regardless of its connection to a particular network (i.e., used in the authentication process, step number 3 in Figure 2). The ability of the proposed system to scale effortlessly enables it to handle a large number of users and devices simultaneously without any significant impact on the system's performance. This feature makes the proposed system an excellent choice for organizations that require a scalable security system to manage their growing user base without compromising the system's reliability or performance.

C. LIMITATION AND CONTINGENCY

In situations where a user cannot access his/her mobile device or there are no APs in their vicinity, the proposed system offers a one-time login solution. This solution requires the user to provide his/her username and answer a security question. Upon successful completion, a one-time Password (OTP) is sent to the user's registered email address, which they can use to access resources granted through the authentication entity.

Although this solution goes against the proposed system's fundamental requirement of not requiring user interaction, it is intended to be used only in rare cases when the user does not have access to his/her mobile device. In typical settings, this should not be a common occurrence. Hence, the one-time login solution serves as a backup mechanism

for cases where the user cannot access his/her mobile device.

The one-time login solution ensures that users can access resources even when they are not near an AP or do not have access to his/her mobile device. As a result, it enhances the user experience by reducing potential downtime and frustration caused by technical limitations.

VIII. CONCLUSION

This paper introduces a Two-factor Authentication (2FA) system that leverages radio waves and Machine Learning (ML) to create an efficient and reliable user authentication process. The proposed system can adapt to different environments and locations and can be customized to meet the specific security needs of a protected entity. The system's parameters, such as the number of Wi-Fi Access Points (APs) and distance threshold, can be adjusted to fit the desired level of security. The proposed system does not require any specialized hardware or infrastructure, making it cost-effective and easy to maintain.

The system also uses a "zero-effort" approach, automating the authentication process and reducing the risk of human error while enhancing user experience and security. Moreover, the continuous authentication feature verifies the user's identity constantly and terminates the session if the devices (i.e., a login device and a mobile device) are no longer in the same location, further improving security and user convenience.

Future research might include a thorough evaluation of the system's performance under various practical scenarios, such as public places, hospitals, offices, and government buildings, to better understand the system's capabilities and limitations. Investigation into how to integrate the proposed system with existing systems, such as access control systems, and how to make the system more scalable and efficient would also be useful for practical implementation and cost optimization.

REFERENCES

[1] ITRC. (2022). *Identity Theft Resource Center's 2021 Annual Data Breach ReportSets New Record for Number of Compromises-Idtheftcenter.org.* [Online]. Available: https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annualdata-breach-report-sets-new-record-for-number-of-compromises/

[2] A. G. J. Cipriani. (2020). *Google Signs Up 150 Million People for Two-Factor Authentication: What it is, How it Works—CNet.Com.* [Online]. Available: https://www.cnet.com/tech/services-and-software/google-signs-up-150-million-people-for-two-factor-authentication-what-it-is-how-it-works/

[3] M. Maynes. (2019). *One Simple Action You Can Take to Prevent 99.9 Percent of Attacks on Your Accounts—Microsoft.Com.* [Online]. Available: https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simpleaction-you-can-take-to-prevent-99-9-percent-of-account-attacks/

[4] C. P. Alto and S.-B. Wire-Yubico. (2020). *Yubico and Ponemon Institute Release the 2020 State of Password and Authentication Security Behaviors Report—Businesswire.Com.* [Online]. Available: https://www.businesswire.com/news/home/20200219005336/en/Yubico-and-Ponemon-Institute-Release-the-2020-State-of-Password-and-Authentication-Security-Behaviors-Report

[5] J. Zhang, X. Tan, X. Wang, A. Yan, and Z. Qin, "T2FA: Transparent two-factor authentication," *IEEE Access*, vol. 6, pp. 32677–32686, 2018.

[6] Y. Oren and D. Arad, "Toward usable and accessible two-factor authentication based on the piezo-gyro channel," *IEEE Access*, vol. 10, pp. 19551–19557, 2022.

[7] E. Hong, S. Lee, M.-K. Oh, and S.-H. Seo, "Two-factor device DNA-based fuzzy vault for industrial IoT device security," *IEEE Access*, vol. 9, pp. 99009–99023, 2021.

[8] A. A. S. AlQahtani, Z. El-Awadi, and M. Min, "A survey on user authentication factors," in *Proc. IEEE 12th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Oct. 2021, pp. 0323–0328.

[9] A. A. S. AlQahtani and T. Alshayeb, "Zero-effort two-factor authentication using Wi-Fi radio wave transmission and machine learning," in *Proc. IEEE 13th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Mar. 2023, pp. 0313–0318.

[10] S.-K. Kim, C. Y. Yeun, E. Damiani, and N.-W. Lo, "A machine learning framework for biometric authentication using electrocardiogram," *IEEE Access*, vol. 7, pp. 94858–94868, 2019.

[11] H. Aksu, A. S. Uluagac, and E. S. Bentley, "Identification of wearable devices with Bluetooth," *IEEE Trans. Sustain. Comput.*, vol. 6, no. 2, pp. 221–230, Apr. 2021.

[12] S. Mondal and P. Bours, "Person identification by keystroke dynamics using pairwise user coupling," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1319–1329, Jun. 2017.

[13] J. Zhang and Q. Zhang, "Comment on 'secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs,'" *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1037–1038, 2023.

[14] W.-H. Lee and R. B. Lee, "Implicit smartphone user authentication with sensors and contextual machine learning," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2017, pp. 297–308.

[15] B. B. Gupta, V. Prajapati, N. Nedjah, P. Vijayakumar, A. A. A. El-Latif, and X. Chang, "Machine learning and smart card based two-factor authentication scheme for preserving anonymity in telecare medical information system (TMIS)," *Neural Comput. Appl.*, vol. 35, no. 7, pp. 5055–5080, Mar. 2023.

[16] P. Punithavathi, S. Geetha, M. Karuppiah, S. H. Islam, M. M. Hassan, and K.-K.-R. Choo, "A lightweight machine learning-based authentication framework for smart IoT devices," *Inf. Sci.*, vol. 484, pp. 255–268, May 2019.

[17] M. Abuhamad, T. Abuhmed, D. Mohaisen, and D. Nyang, "AUToSen: Deep-learning-based implicit continuous authentication using smartphone sensors," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5008–5020, Jun. 2020.

[18] K. Lee, C. Esposito, and S.-Y. Lee, "Vulnerability analysis challenges of the mouse data based on machine learning for image-based user authentication," *IEEE Access*, vol. 7, pp. 177241–177253, 2019.

[19] C. Tang, Z. Cui, M. Chu, Y. Lu, F. Zhou, and S. Gao, "Piezoelectric and machine learning based keystroke dynamics for highly secure user authentication," *IEEE Sensors J.*, Jan. 2022.

[20] R. Nadia, B. A. Tama, and J. Song, "Seamless human impedance-based IoT authentication with machine learning techniques," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2020, pp. 339–343.

[21] N. Djosic, B. Nokovic, and S. Sharieh, "Machine learning in action: Securing IAM API by risk authentication decision engine," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2020, pp. 1–4.

[22] P. Bhattacharya, C. Trivedi, M. S. Obaidat, K. Patel, S. Tanwar, and K.-F. Hsiao, "BeHAutH: A KNN-based classification scheme for behavior-based authentication in web 3.0," in *Proc. Int. Conf. Commun., Comput., Cybersecurity, Informat. (CCCI)*, Oct. 2022, pp. 1–5.

[23] L. Xiao, X. Lu, T. Xu, W. Zhuang, and H. Dai, "Reinforcement learning-based physical-layer authentication for controller area networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2535–2547, 2021.

[24] G. Oligeri, S. Sciancalepore, S. Raponi, and R. D. Pietro, "PAST-AI: Physical-layer authentication of satellite transmitters via deep learning," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 274–289, 2023.

[25] M. Agrawal, P. Mehrotra, R. Kumar, and R. R. Shah, "Defending touch-based continuous authentication systems from active adversaries using generative adversarial networks," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Aug. 2021, pp. 1–8.

[26] A. Acar, H. Aksu, A. S. Uluagac, and K. Akkaya, "A usable and robust continuous authentication framework using wearables," *IEEE Trans. Mobile Comput.*, vol. 20, no. 6, pp. 2140–2153, Jun. 2021.

[27] T. Zhao, Y. Wang, J. Liu, Y. Chen, J. Cheng, and J. Yu, "True-Heart: Continuous authentication on Wrist–Worn wearables using PPG-based biometrics," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Jul. 2020, pp. 30–39.

[28] P. Lyu, W. Cai, and Y. Wang, "Continuous authentication against collusion attacks," *Sensors*, vol. 22, no. 13, p. 4711, Jun. 2022.

[29] T. Zhao, Y. Wang, J. Liu, J. Cheng, Y. Chen, and J. Yu, "Robust continuous authentication using cardiac biometrics from Wrist–Worn wearables," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9542–9556, Jun. 2022.

[30] Y. He, W. Wang, Y. Teng, Q. Wang, M. Wang, and J. Lin, "ABLE: Zero-effort two-factor authentication exploiting BLE co-location," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2022, pp. 992–997.

[31] 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.

[32] B. Shrestha, M. Mohamed, and N. Saxena, "ZEMFA: Zero-effort multi-factor authentication based on multi-modal gait biometrics," in *Proc. 17th Int. Conf. Privacy, Secur. Trust (PST)*, Aug. 2019, pp. 1–10.

[33] E. Husa and R. Tourani, "Vibe: An implicit two-factor authentication using vibration signals," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2021, pp. 236–244.

[34] Z. A. Atallah, P. S. JosephNg, and K. Y. Phan, "JomNFC: Zero effort intelligent access system," in *Proc. Innov. Power Adv. Comput. Technol. (I-PACT)*, Nov. 2021, pp. 1–6.

[35] M. Agrawal, P. Mehrotra, R. Kumar, and R. R. Shah, "GANTouch: An attack-resilient framework for touch-based continuous authentication system," *IEEE Trans. Biometrics, Behav., Identity Sci.*, vol. 4, no. 4, pp. 533–543, Oct. 2022.

[36] L. Déncs-Fazakas, E. Kail, and R. Fleiner, "Two-factor, continuous authentication framework for multi-site large enterprises," in *Proc. IEEE 20th Int. Symp. Comput. Intell. Informat. (CINTI)*, Nov. 2020, pp. 173–178.

[37] I. Lamiche, G. Bin, Y. Jing, Z. Yu, and A. Hadid, "A continuous smartphone authentication method based on gait patterns and keystroke dynamics," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 11, pp. 4417–4430, Nov. 2019.

[38] S. Almohamade, J. Clark, and J. Law, "Continuous user authentication for human-robot collaboration," in *Proc. 16th Int. Conf. Availability, Rel. Secur.*, 2021, pp. 1–9.

[39] R. Li, H. Liao, J. An, C. Yuen, and L. Gan, "Intra-class universal adversarial attacks on deep learning-based modulation classifiers," *IEEE Commun. Lett.*, vol. 27, no. 5, pp. 1297–1301, May 2023.

[40] Flaticon. (2023). *Flaticon: Free Vector Icons*. 40 Flaticon. [Online]. Available: https://www.flaticon.com

THAMRAA ALSHAYEB received the B.S. degree in physics from King Khalid University, and the M.S. degree in applied physics, the M.S. degree in electrical engineering, and the Ph.D. degree in engineering physics from Louisiana Tech University, in 2020. She is currently an Assistant Professor with George Mason University. Prior to that, she was with the University of Wisconsin-Green Bay and North Carolina Agricultural and Technical State University. She was also a Research Associate with the U.S. Department of Energy, Jefferson Lab. Her research interests include nuclear physics, nuclear physics data analysis, nanotechnology, electromagnetic radiation, educational physics, and ML applications.

MAHMOUD NABIL (Member, IEEE) received the Bachelor of Science (B.S.) and Master of Science (M.S.) degrees (Hons.) in computer engineering from Cairo University, Egypt, in 2012 and 2016, respectively, and the Ph.D. degree in electrical and computer engineering from Tennessee Tech University, Cookeville, TN, USA, in 2019. Currently, he holds the position of an assistant professor with the Department of Electrical and Computer Engineering, North Carolina Agricultural and Technical State University. He is an Accomplished Researcher. He has authored and coauthored numerous publications in prestigious venues. His research work has been published in renowned journals, such as IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON HUMAN-MACHINE SYSTEMS, and IEEE TRANSACTIONS ON MOBILE COMPUTING. He has also contributed to leading conferences, including the International Conference on Communication, the International Conference on Pattern Recognition, and the International Conference on Wireless Communication. With diverse research interests, his areas of expertise include security and privacy in unmanned aerial systems, smart grids, machine learning applications, vehicular ad hoc networks, and blockchain applications. He has received significant funding for his research projects from esteemed national agencies and organizations, including the National Science Foundation (NSF), the Department of Transportation (DOT), the Air Force Research Laboratory (AFRL), NASA, Intel, Cisco, and Lockheed Martin.

ALI ABDULLAH S. ALQAHTANI (Member, IEEE) received the B.S. degree (summa cum laude) in computer science, the M.S.Eng. degree in electrical engineering, the M.S. degree in computer and information science, with a focus on cybersecurity and privacy, and the Ph.D. degree in engineering-cyberspace engineering.

He is currently an Assistant Professor of computer systems technology and the Founding Director of the CyberNex Research Laboratory. Prior to this, he was an Assistant Professor of computer science with the University of Wisconsin-Green Bay and an Assistant Professor of cybersecurity with the University of Wisconsin Extended Campus. His primary research interests include advancing cybersecurity, particularly in the area of digital authentication. He develops innovative, zero-effort authentication methods that seamlessly integrate into the digital ecosystem, balancing enhanced security with user convenience. Moreover, his work includes threat identification and security analysis, targeting vulnerabilities both inside and outside organizational frameworks. Additionally, he explores the vast potential of the Internet of Things (IoT) and harnesses the power of artificial intelligence (AI) and machine learning (ML) across various fields.

AHMAD PATOOGHY (Senior Member, IEEE) received the Ph.D. degree in computer engineering from the Sharif University of Technology, Tehran, Iran, in 2011. From 2011 to 2017, he was an Assistant Professor with the Iran University of Science and Technology, Tehran. Then, he joined the University of Central Arkansas, Conway, AR, USA, from 2018 to 2021. Since August 2021, he has been with the Department of Computer Systems Technology, North Carolina Agricultural and Technical State University, and leading the Intelligent Cyber-Systems and Architectures Laboratory. He has published more than 100 peer-reviewed journal articles and conference proceedings. His research interests include the security and reliability of machine learning applications and accelerators, hardware security in the IoT and cyber-physical systems, and hardware design for machine learning acceleration. He is a Senior Member of IEEE Computer Society and a member of ACM. He has been a Reviewer and a PC Member of various IEEE, ACM, Elsevier, and Springer journals and conferences. He has also served as a Panelist for the National Science Foundation for reviewing grant proposals.

• • •