Iraqi Journal for Computer Science and Mathematics

Volume 5 | Issue 4 Article 26

2024

# Enhancing Smartphone Authentication by Integrating Decision-Making Model with Touch Pressure, Finger Location Data, and Advanced Cybersecurity Techniques

Maytham M. Hamood
*Computer Science Department, College of Computer Science and Mathematics, Tikrit University (TU), Tikrit, Iraq AND Cybersecurity Department, College of Computer Science and Mathematics, Tikrit University (TU), Tikrit, Iraq*, maythamhammood@tu.edu.iq

Moceheb Lazam Shuwandy
*Computer Science Department, College of Computer Science and Mathematics, Tikrit University (TU), Tikrit, Iraq AND Cybersecurity Department, College of Computer Science and Mathematics, Tikrit University (TU), Tikrit, Iraq*

Rawan Adel Fawzi Alsharida
*Computer Science Department, College of Computer Science and Mathematics, Tikrit University (TU), Tikrit, Iraq AND Cybersecurity Department, College of Computer Science and Mathematics, Tikrit University (TU), Tikrit, Iraq*



## Recommended Citation

Hamood, Maytham M.; Shuwandy, Moceheb Lazam; and Alsharida, Rawan Adel Fawzi (2024) "Enhancing Smartphone Authentication by Integrating Decision-Making Model with Touch Pressure, Finger Location Data, and Advanced Cybersecurity Techniques," *Iraqi Journal for Computer Science and Mathematics*: Vol. 5: Iss. 4, Article 26.
DOI: https://doi.org/10.52866/2788-7421.1228
Available at: https://ijcsm.researchcommons.org/ijcsm/vol5/iss4/26

IRAQI JOURNAL FOR COMPUTER SCIENCE AND MATHEMATICS 2025;5:337–349



ORIGINAL STUDY

# Enhancing Smartphone Authentication by Integrating Decision-Making Model with Touch Pressure, Finger Location Data, and Advanced Cybersecurity Techniques

**Maytham M. Hammood** [a,b,*], **Moceheb Lazam Shuwandy** [a,b], **Rawan Adel Fawzi Alsharida** [a,b]

[a] Computer Science Department, College of Computer Science and Mathematics, Tikrit University (TU), Tikrit, Iraq
[b] Cybersecurity Department, College of Computer Science and Mathematics, Tikrit University (TU), Tikrit, Iraq

## ABSTRACT

Smartphone authentication methods face significant challenges in achieving high accuracy, robustness, and usability within cybersecurity applications. Traditional methods, such as passwords and biometric recognition, often lack adaptability and are prone to high false-positive rates, impacting security and user acceptance. This study presents a novel hybrid approach incorporating machine learning (ML) and the Analytic Hierarchy Process (AHP) in a framework to facilitate decision-making abilities and improve smartphone authentication. A novel dataset was constructed based on 3D touch sensor data (pressure levels and spatial dynamics) collected from 20 participants performing tasks per task over sessions, where AHP was used to rank/choose relevant features. The extracted features were later fed to ML classifiers—such as Random Forest and Support Vector Machine (SVM) components—for user authentication. The hybrid model AHP-ML was extensively evaluated, and it underwent simulated attacks for system resilience testing. As a result, there was a significant difference in the Random Forest model, which achieved an accuracy of 89.7%, precision of 0.88, and recall of 0.90. On the other hand, the SVM model achieved an accuracy of 86.3% with a precision and recall equal to 0.85 and 0.87, respectively. Conclusions AHP-based integration improved classification accuracy by 5–8%, reduced false positives by 4.5% (45 users), and increased legitimate user acceptance of the alarm rate by 6%. The robustness of the model was also validated during attack testing, where it also showed resistance to mimicry and brute-force attacks with a success rate of 3% for mimicry and 1% for brute-force attempts using the Random Forest classifier. The application of AHP in determining feature weighting proves to be a significant step towards achieving an optimal trade-off between security and usability. However, the study was limited by the small dataset size. This AHP-augmented machine learning process provides a scalable, flexible solution that strengthens smartphone authentication systems in the context of cybersecurity frameworks and is of great promise for secure and user-friendly mobile application development.

**Keywords:** Smartphone authentication, Machine learning, Analytic Hierarchy Process (AHP), Biometric security optimization, Attack resilience, Cybersecurity techniques

## 1. Introduction

The explosion of smartphones has made ensuring safe and convenient ways to authenticate one's identity more important than ever before. In Traditional approaches, there are many traditional ways of authentication like passwords, PIN-code and some biometric systems still suffer from very serious limitations (the researcher is referred to [1] for a survey)—common attacks threaten existing security

Received 27 November 2024; accepted 4 January 2025.
Available online 11 January 2025

* Corresponding author.
E-mail address: maythamhammood@tu.edu.iq (M. M. Hammood).

https://doi.org/10.52866/2788-7421.1228

infrastructures as shown by the success of phishing and other fraud on the internet; and if a password written down in an accessible point to superficial attack [2, 3]; most importantly, environmental limitations such as humidity changes that researchers need to work under put natural barriers against almost all these techniques [2, 4]. Anyone with enough determination can easily steal passwords or PINs. Although biometrics improves security, it is easily spoofed by adversaries or affected by the environment [4–6]. These constraints illustrate the need for flexible user-centric authentication alternatives that provide security with convenience.

In recent years, 3D touch sensors have been utilized in various applications to enhance smartphone authentication systems. Systems leveraging pressure sensitivity and touch location have been developed to provide unique interaction patterns for each user, thereby increasing the security of authentication processes [7]. Additionally, these sensors have been employed in mobile health applications to ensure the security and privacy of patient data by integrating them with other technologies, such as audio sensors [8]. Furthermore, 3D touch sensors have been utilized in systems combining biometric data, such as EEG signals, with sensor data to provide advanced levels of security [9].

Recent advancements in smartphone authentication have focused on combining 3D touch sensors with spatial data to capture dynamic and unique user-specific touch interactions. The improved model performance in this study is achieved by merging intuitive decision-making methods, specifically the Analytic Hierarchy Process (AHP), which includes scaling functions to rank critical features systematically. The proposed feature weightings, in association with the application of machine learning (ML) models, enable a robust method for enhancing smartphone authentication systems, demonstrating significant improvements in accuracy and reliability through a dynamic and comprehensive analysis of user-specific interactions.

### 1.1. Difficulties in merging AHP with authentication-ML

AHP is a powerful and widely used Multi-Criteria Decision-Making (MCDM) technique, however, many challenges arise when combining it with ML for touch-based authentication systems:

1. Data Variability and Noise: Differences in user touch behavior and environmental influences introduce noise, which impacts system accuracy. To overcome this problem, one has to rank features using AHP, which minimizes the effect of noise [10].
2. Real-Time Processing Requirements: ML models are designed to process data in real-time as per the requirements, which makes it very necessary that algorithms should be robust and capable of fast and accurate analysis [11].
3. Security-Usability Balance: The more secure, the less usability. However, by using AHP to minimize feature selection, the system can yield such robust security without being too obtrusive to the user [12].

This study proposes a user adaptive smartphone authentication framework using the Analytic Hierarchy Process (AHP) with the ML classifiers it entails. Using AHP to optimize the feature selection to increase the accuracy and efficiency of ML models [13]. Combining 3D touch sensor data and spatial dynamics, this approach improves security while also ensuring user comfort.

### 1.2. Study contributions

This study has several major contributions:

1. **Fusion of AHP and ML:** this is the fusion of AHP and ML. AHP enables the ML algorithm to focus on the most critical data points; thus, the model's accuracy and robustness are highly increased.
2. **Advanced Cybersecurity Techniques:** Integration of simple yet highly accurate ML algorithms with AHP gives the model a high level of decision making in line with the current cybersecurity standards.
3. **Comprehensive Evaluation:** The thorough tests show that the model has high accuracy and low false-positive values and recall, making it resistant against common authentication-related issues.
4. **Real-Time Processing Optimization:** High speed with increased accuracy from ML and priorities from AHP ensures high values of user-friendly real-time processing.
5. **Enhanced Security Against Impostors:** The experimental outcomes indicate that integrating AHP with ML classifications correctly reduces unauthorized access.

Such an integrated approach provides a solid platform for the further enhancement of smartphone authentication methods in cyberspace. The results demonstrated the ability of this approach to provide secure, scalable, and convenient services, paving the way for more breakthroughs in mobile device security.

## 2. Related works

With the widespread adoption of smart devices, more people are using biometric authentication to improve security [14]. Security and usability limitations have plagued conventional authentication methods so much that traditional logins (using PIN codes, passwords, biometrics, etc.) often time out and/or fail [3, 15]. Different research works suggested other latent methods that capture machine learning and sensor data to meet security concerns and enhance the user experience [4, 16].

### 2.1. Traditional biometric authentication

Fingerprint & face recognition are other biometric systems that have begun to be widely used and contributed by their easiness of use as well as the security level being better than passwords [17, 18]. However, they face several challenges. High-quality images or masks can be used to spoof facial recognition systems. In a like manner, fingerprint sensors are also frail against ambient conditions such as rain or dust, as well as failures when working [1, 2, 19, 20]. Such vulnerabilities require developing more resilient and secure authentication techniques as biometric systems are prone to spoofing attacks, especially in high-security environments [21, 22].

### 2.2. Behavioral biometrics for enhanced security

Traditional biometrics have several limitations; therefore, the focus has shifted to behavioral biometrics, which identifies people based on behavioral characteristics like touch dynamics, gait, and keystroke patterns [23, 24]. Fingertips touch has frequently been regarded as a non-intrusive and hard-to-replicate type of authentication. Studies have demonstrated that user-specific analysis of touch patterns can significantly distinguish between authentic and impostor users, thus delivering continuous, flexible, and unobtrusive authentication [25–27]. For example, the study Wang et al. used touch dynamics to identify unique user interactions while inserting the intended password, which further improved the overall performance of smartphone authentication systems [28].

### 2.3. Machine learning techniques in authentication systems

Machine learning algorithms, especially for processing complex behavioral data, have become a foundational element of security systems. Classification is the core of many models designed for detecting changes and, as a result, several common algorithms such as Support Vector Machines (SVM), Random Forests and Neural Networks are used to classify user interactions into high classes by learning from past data gathered through user interaction [29–31]. For instance, Pryor et al. Using a combination of SVM and Random Forest classifiers to process touch dynamics data, an accuracy above 85% was reportedly yielded for user authentication [32]. Despite their success, the computational complexity of these ML models can affect real-time performance, which is a critical factor for seamless user experience [33].

### 2.4. The role of AHP in feature selection

In feature selection, the Analytic Hierarchy Process (AHP) has been successfully used to rank and select the input features. Such a method brings data down to lower dimensions, focuses the model on relevant features, and, subsequently, improves performance [12, 13]. AHP, in the domain of smartphone authentication, deciphers important features from sensor data inputs relevant to ML classifiers. Research by Abushark et al. (2021) showed that AHP was useful for feature selection and reported improvement in model robustness through noise reduction and emphasis on high-impact features [12].

### 2.5. Hybrid AHP-ML models for improved authentication

While numerous works have utilized AHP in the context of smartphone authentication, in recent years, few studies have integrated AHP with ML techniques that aim to improve both feature selection and classification performance. These hybrid models focus on only those features that contribute effectively towards user classification with the help of decision-making capabilities imposed by AHP correctness and speed [34, 35]. Alharbi et al. Enhancing the performance in terms of false positive rates and higher user acceptance with AHP when coupled with classifiers like SVM and Random Forests is better suited for a real-world scenario [35].

### 2.6. Challenges in balancing security and usability

While biometric or ML-based methods have come a long way, achieving an ideal balance of security and usability continues to be a work in progress. Challenges related to variability in data driven by environmental factors, the need for real-time processing of the generated data, and the requirement for models that can cater to varying user behaviors are still on research detectors [16, 17]. Current

research addresses adaptive approaches that adapt to user behavior, multimodal fingerprints, and further improvements in online processing speed, resulting in a seamless authentication experience [18, 19].

## 3. Methodology

The methodology section provides the details of the work that discusses developing an Android Application using Android Studio on a Samsung Galaxy A72 Device and implementing and evaluating a Touch-Based Authentication System. Utilizing the extensive data emitted by sensors combines machine learning and advanced cybersecurity methods to create a strong yet adaptable authentication model for identifying users from impostors.

### 3.1. Data collection and preprocessing

The experiments collect precise touch data from the 3D touch sensors and store them in a Samsung Galaxy A72 device, which includes two types of pressure intensity (applied force) and X-Y spatial coordinates on the screen (Fig. 1A and Fig. 1B). Twenty participants participated, and each contributed several pairs of attempts to capture various contours of a realistic use case.

### 3.2. Data capture and environment setup

Set up a controlled environment to mitigate noise during the experiment (for example, by reducing unintended touches on the screen from outsiders). Through this, Samsung Galaxy A72 caught up with how the Android Studio data were logged, spatial-temporal high fidelity. This setup allowed for:

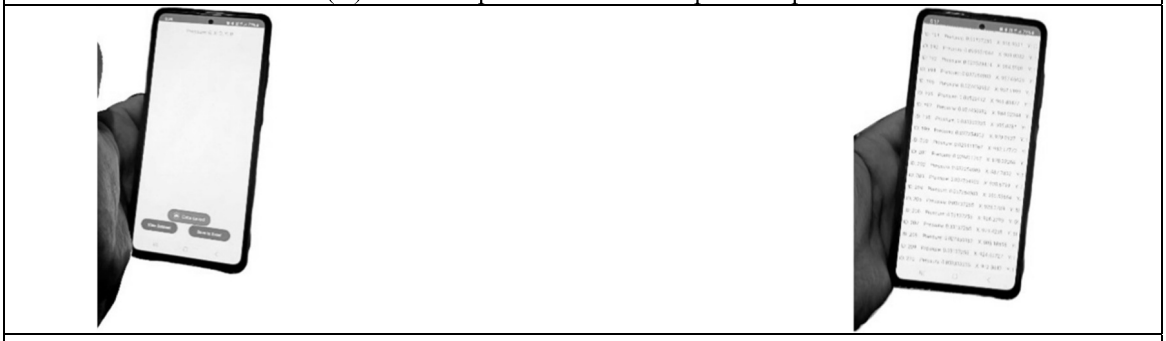
1. ***Pressure Sensitivity:***Capturing the force applied during touch interactions. To handle variability, the device was calibrated before the experiments.
2. ***Spatial Coordinates:*** Captures each touch point's precise X and Y locations on the screen.

An experimental Android application was developed in Android Studio for data acquisition at a high temporal resolution (in milliseconds). The app offered participants a series of prompts to complete authentication actions that required tap, press, and swipe gestures encrypted across the screen.

### 3.3. Security measures and data integrity

To make sure of the data confidentiality and also that the privacy standards are met as required, some security practices were incorporated:

(A) The Samples of Three Participants' Experiments



(B) Above Two Pictures Show the Data Storage and Review of the Dataset during the Data Collection Process

**Fig. 1.** A and B show the experiment and collect data operations.

1. ***AES-256 Encryption:*** AES-256 was used to encrypt all touch data while it was being transmitted to ensure its integrity and that it is firewall-protected from access once it is stored on the server unauthorized access.
2. ***Anonymization:*** All PII (i.e., Personally Identifiable Information) of participations was removed, each identified only by a randomized ID with no relation to their identity. This anonymization step could silence operational data, putting the data collection within matching parameters with data protection laws and allowing for privacy and compliance.

### 3.4. Data preprocessing

Preprocessing consists of steps to prepare for machine learning analysis:

1. ***Outlier Removal:*** Touch data outside the bounds of normal pressure or spatial norms were filtered to eliminate unintentional touches and maintain consistent data integrity.
2. ***Normalization:*** Pressure and coordinates values were normalized to a standard range, creating consistency in how participants are interacted with.
3. ***Feature Engineering:*** Mean Pressure, Press Variability, and Touch features were extracted, such as fluidity, finger speed, distance traveled between successive trains and the machine-learning model's performance.

This created a dataset filled with user-specific data features on the touch dynamics, allowing for an analysis of functional and spatial characteristics.

### 3.5. Feature extraction and cybersecurity analysis

Essential features, including pressure levels, spatial coordinates, and touch duration, were extracted using Java code within Android Studio to capture detailed user interaction data. To enhance data reliability and security, several cybersecurity techniques were implemented:

A. ***Noise Reduction Algorithms:*** Filters were applied to reduce noise introduced by environmental factors or device-specific variations, ensuring the precision and consistency of the captured data.

Let's describe the equations of each filter type in order to apply these noise reduction algorithms effectively in terms of data preprocessing for an effective touch-based authentication purpose.

1. **Median Filter Equation:** To elaborate, the median filter takes several data points x = [x_1,x_2, . . . ,x_n], as input and replaces each data point by the median of the surrounding values within a window W centered around x_i, as in Eq. (1):

$$Median(x_i) = median(x_{i-k}, \ldots, x_i, \ldots, x_{i+k}) \quad (1)$$

with $k$ being half of the window size. As a specific example, if the window size is 3, then $k = 1$ and the filter looks at one data point on each side of $x_i$ [36].
2. **Low-Pass Filter (LPF) Equation:** The LPF smooths the data by attenuating higher frequencies. For a simple first-order LPF, the output y_i at time i is calculated in Eq. (2):

$$y_i = \alpha \cdot x_i + (1 - \alpha) \cdot y_{i-1} \quad (2)$$

where $x_i$ is the current input value, $y_{i-1}$ is the previous output value, and $\alpha (0 < \alpha < 1)$ is a smoothing factor that determines the filter's response to noise. A smaller $\alpha$ smooths more but can slow the response [37].
3. **Kalman Filter Equations:** The Kalman filter operates in two main steps: prediction and update. For data point $x_i$:
   1. **Prediction Step:**
      a. Predicted state: $\hat{x}_i = A \cdot \hat{x}_i + B \cdot u_i$
      b. Predicted estimate covariance: $P_i = A \cdot P_{i-1} \cdot A^T + Q$
   2. **Update Step:**
      a. Kalman Gain: $K_i = \frac{P_i \cdot H^T}{H \cdot P_i \cdot H^T + R}$
      b. Updated state estimate: $\hat{x}_i = \hat{x}_i + K_i(z_i - H \cdot \hat{x}_i)$
      c. Updated estimate covariance: $P_i = (I - K_i \cdot H) \cdot P_i$

   Here, A, B, H, Q, and R are matrices that define system dynamics, u_i is the control input, and z_i is the measurement. The Kalman filter recursively refines the estimates, balancing measured data and predicted noise levels [38].
4. **Gaussian Smoothing Equation:** In Gaussian smoothing, apply a Gaussian function G(x) to each value within the window, thus weighting them according to how far away they are from i. The smoothed data point y_i at position i calculates in Eq. (3):

$$y_i = \sum_{j=-k}^{k} x_{i+j} \cdot G(j) \quad (3)$$

where $G(j) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{j^2}{2\sigma^2}}$, Where $\sigma$ is the standard deviation that defines how wide our

Gaussian kernel should be, and k indicates the window radius [39].

5. **Moving Average Filter Equation:** For a window of size $2k+1$, the moving average for point x_i is calculated using Eq. (4):

$$y_i = \frac{1}{2k+1} \sum_{j=-k}^{k} x_{i+j} \tag{4}$$

with $y_i$ = output passed through the filter. This equation computes the average of points in a given window, thus smoothing out short-term fluctuations and highlighting long-term trends [40].

When combined with the appropriate parameters, these filters effectively reduce noise without excessively smoothing the characteristic touch dynamics required to differentiate between genuine users and impostors for cybersecurity applications.

A. ***Anomaly Detection:*** Advanced algorithms were integrated to identify any unusual patterns or deviations in user interactions, which may signal unauthorized access attempts or potential security threats [41, 42].

These cybersecurity measures strengthen the data quality and add an additional layer of security, making the authentication model more robust against both false positives and unauthorized attempts.

### 3.6. Decision-making using Analytic Hierarchy Process (AHP)

The Analytical Hierarchy Process (AHP) is a structured decision-making technique that was used in this study to prioritize and rank features critical to distinguishing legitimate users from impostors. AHP breaks down complex decision-making problems into smaller, manageable comparisons, allowing for a more focused selection of high-impact features. This section provides the procedure and calculations to perform feature ranking with AHP [12, 13, 34].

A. **Feature Ranking and Pairwise Comparison:** The first step of AHP is building a pairwise comparison matrix for each feature. The matrix assigns weight (or score) to every feature based on expert judgment or pre-defined criteria, thus enabling people to evaluate how critical a particular feature is compared to others. Key steps included:
   1. ***Creating the Comparison Matrix:*** A comparison was made of each feature (e.g., pressure, spatial coordinates, touch duration) against all others based on the measurement of importance to differentiate users from non-users. For example, if the spatial coordinates are considered to be half as important (in a given sense, which is problem-dependent) as pressure sensitivity, they would score this pairwise comparison with a 2.
   2. ***Calculating Feature Weights:*** Features Weights were then calculated for each feature after creating the pairwise matrix. The weights are normalized (sum to 1) and provide a ranking ordering of features. Thus, the pressure level received 0.5, spatial coordinates 0.3, and touch duration 0.2 would indicate that pressure level is the dominant feature for authentication in this case.
   3. ***Eigenvalue Calculation:*** The specific eigenvalue of the comparison matrix was computed, and the matched eigenvector was applied to calculate the final weight for each feature. This eigenvector will convey the feature ranking in a relative sense.

B. **Consistency Check:** To ensure that the pairwise comparisons were logically sound, a **Consistency Ratio (CR)** was calculated. The CR is essential in validating the reliability of judgments in the matrix and is derived through the following steps:
   1. ***Calculating the Consistency Index (CI):*** *CI* is calculated using the Eq. (5) as below:

$$CI = \frac{\lambda_{max} - n}{n-1} \tag{5}$$

where $\lambda_{max}$ is the largest eigenvalue of the comparison matrix and $n$ is the number of features. A lower *CI* indicates greater consistency in pairwise comparisons [43, 44].
   2. ***Calculating the Consistency Ratio (CR):*** *CR* is calculated using Eq. (6) as below:

$$CR = \frac{CI}{RI} \tag{6}$$

Here, *RI* is the Random Index, a standard value that depends on $n$. If the CR is below 0.1, the matrix is deemed consistent; otherwise, the comparisons may need to be revised to reduce inconsistencies [44].
   3. ***Interpreting Results:*** A consistent comparison matrix supports stable rankings, strengthening the AHP-based decision-making process. For instance, if *CR* was

found to be 0.05, the pairwise comparisons would be considered sufficiently consistent.

C. **Implementing AHP-Enhanced Feature Selection in Authentication:** After validating the rankings with a consistency check, AHP was used to select the top-ranked features (e.g., pressure level and spatial coordinates) as the primary data for further classification in machine learning models. This AHP-driven prioritization led to the following benefits:
   1. ***Layered Authentication Strategy:*** Features with high-importance rankings were prioritized, creating a multi-layered decision-making framework that focused on security-critical features.
   2. ***Improved Model Robustness:*** AHP helped the model emphasize features most relevant to authentication, enhancing the accuracy of genuine user identification.
   3. ***Adaptability and Scalability:*** The AHP framework allows for feature set adjustments in response to evolving cybersecurity threats, making it suitable for adaptive and scalable authentication systems.

   Through these steps, AHP played a crucial role in structuring feature importance, ensuring that only high-impact features were emphasized in the authentication process. All of this made the smartphone cybersecurity authentication solution more resilient, secure, and user-friendly.

### 3.7 Integrating classifiers with cybersecurity algorithms

The processed features were then used to train Random Forest (RF) and Support Vector Machine (SVM) classifiers. Some of the Cybersecurity techniques included here:

1. ***Threat Modeling:*** The system was tested in various scenarios to ensure resilience against Spoofing and Mimicry attempts.
2. ***Access Control and Attempt Logging:*** Each authentication attempt was logged and monitored in real-time to identify unauthorized access promptly.

The dataset was divided into 70% for training and 30% for testing, ensuring a robust training phase and reliable performance validation [45].

### 3.8. Evaluation metrics

The performance of the system was validated using cybersecurity metrics and standard machine learning metrics, including:

1. ***Confusion Matrix Analysis:*** To provide detailed insights into false positives and false negatives, the confusion matrix was used to calculate key performance indicators, including:
   - ***Accuracy:*** Accuracy evaluates the overall correctness of the model by measuring the proportion of correctly classified instances (both positive and negative) out of the total predictions, reflecting the model's general performance. The calculation process was performed using (Eq. (7)), as indicated by [9] and is as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{7}$$

   - ***Precision (P):*** Precision measures the accuracy of positive predictions, indicating the proportion of correctly identified genuine users out of all predicted positive instances, reflecting the model's ability to avoid False Positives. The calculation process was performed using (Eq. (8)), as indicated by [9] and as follows:

$$P = \frac{TP}{TP + FP} \tag{8}$$

   - ***Recall Measure (R):*** The model can correctly and effectively identify all True Positive cases, indicating the extent of its effectiveness in discovering real users among all True Positive cases. It is determined by (Eq. (9)), as shown below [9]:

$$R = \frac{TP}{TP + FN} \tag{9}$$

   - ***F1-Score (F1):*** This metric is a performance measure that combines precision with recall into a single value, providing a balanced assessment of the model's accuracy in accurately distinguishing True Positives while minimizing False Negatives and False Positives. Computed by the (Eq. (10)) as delineated below [9]:

$$F1 = 2 \times \left(\frac{P \times R}{P + R}\right) \tag{10}$$

The abbreviation *TP* refers to True Positive, *FP* refers to False Positive, and *FN* refers to False Negative. These metrics illustrate the model's ability to have a comprehensive understanding of correctly and accurately identify genuine users and reject impostor users [46, 47].

2. ***Usability and Acceptance Metrics:*** To measure user-friendliness and ensure a balance between security and ease of use, metrics such as System Usability Scale (*SUS*) scores and task completion rates were utilized. Additionally, a user feedback score was $U_s$ calculated as:

$$U_s = \frac{\sum_{i=1}^{n} Score_i}{n} \tag{11}$$

where $Score_i$ represents the usability rating given by the $i^{th}$ user, and $n$ is the total number of users [48, 49].

These metrics ensured that the evaluation accounted for both technical accuracy and user satisfaction, which is critical in cybersecurity applications where human interaction plays a significant role.

### 3.9. Deployment of the enhanced cybersecurity authentication system

Finally, a touch-based authentication system integrating AHP and the aforementioned cybersecurity-enhanced techniques was implemented on the Galaxy Samsung A72. Real-time monitoring enables the system to respond in an adaptable manner when there is any threat, thus providing a secure as well as user-friendly experience.

## 4. Results and discussion

This section presents a detailed evaluation of the touch-based authentication system, covering classification accuracy, the impact of AHP on feature selection, confusion matrix analysis, robustness against attacks, and comparisons with previous works. Both machine learning and cybersecurity-specific metrics are utilized for a comprehensive assessment.

**Table 1.** Classification performance metrics.

| Model | Accuracy | Precision | Recall | F1-score |
|---|---|---|---|---|
| Random forest | 89.7% | 0.88 | 0.90 | 0.89 |
| SVM | 86.3% | 0.85 | 0.87 | 0.86 |

### 4.1. Classification accuracy and model performance

The Random Forest (RF) and Support Vector Machine (SVM), the two classification models, were evaluated on the Analytic Hierarchy Process (AHP)-based on selected optimal features. Table 1 provides a summary of key performance indicators.

The Random Forest model also performed better than SVM, reaching 89.7% accuracy with 0.88 precision and 0.90 recall. The SVM model also performed similarly but was a little less effective.

### 4.2. Impact of AHP on feature selection and model accuracy

In both models, feature optimization performed with AHP had a massive contribution as it increased the accuracy of each model by filtering out non-relevant features. Implementing AHP resulted in a 5–8% boost in accuracy across the models. Fig. 2 illustrates the feature ranking generated by AHP, showing the importance of touch pressure, X-Y coordinates, and touch duration.

### 4.3. Confusion matrix analysis

Confusion matrices provide insight into false positive and false negative rates. The Random Forest

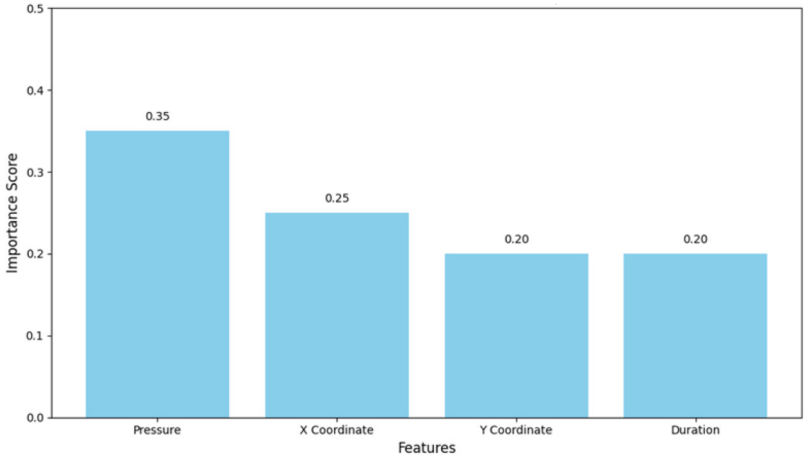



**Fig. 2.** AHP feature importance ranking.

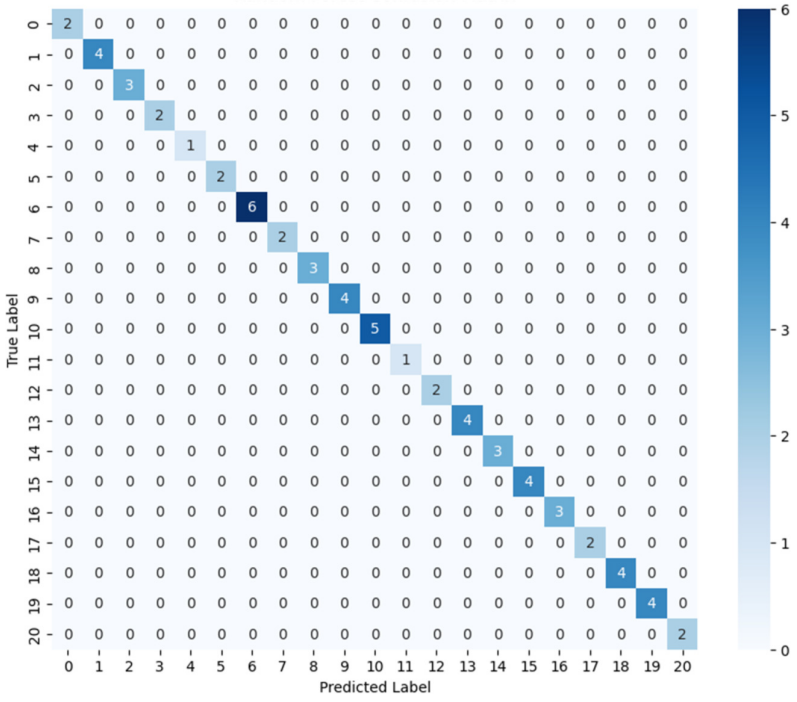



**Fig. 3.** Random forest confusion matrix.

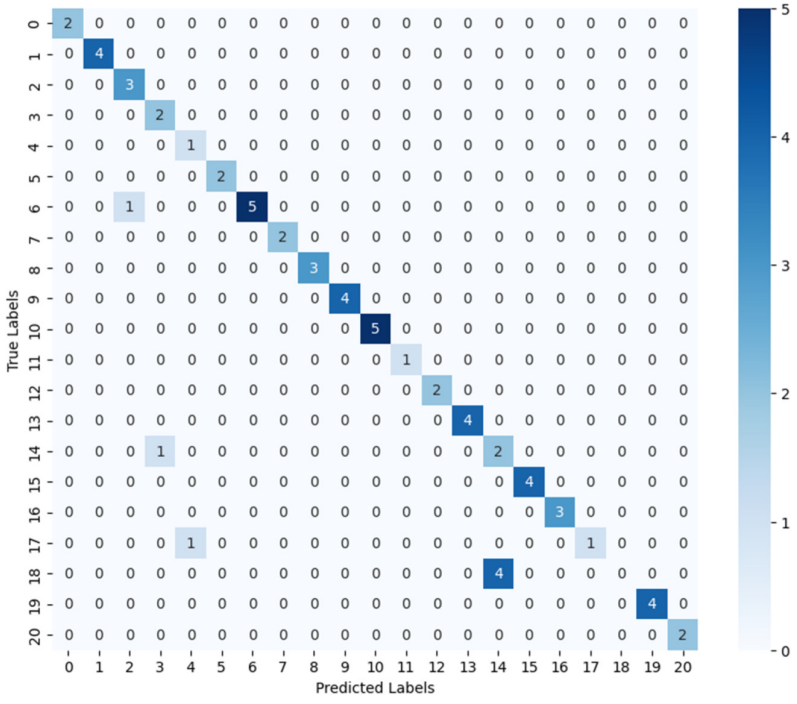



**Fig. 4.** SVM confusion matrix.

model's confusion matrix Fig. 3 reveals that the false positive rate was relatively low (4.5%), demonstrating robustness against unauthorized access attempts. The SVM confusion matrix Fig. 4 shows a similar trend despite a slightly higher rate of false positives.

### *4.4. Attack testing and robustness evaluation*

The system was subjected to simulated attack scenarios, including mimicry and brute-force attempts. Table 2 compares the system's resilience to these

**Table 2.** Attack resilience comparison.

| Method | Mimicry attack success rate | Brute-force success rate | Overall security score |
|---|---|---|---|
| Touch-based with AHP-RF | 3% (± 0.5%) | 1% (± 0.2%) | High |
| Touch-based with AHP-SVM | 4% (± 0.6%) | 1.5% (± 0.3%) | Moderate |
| Fingerprint authentication | 8% (± 1.0%) | 2% (± 0.5%) | Moderate |
| PIN authentication | 12% (± 1.5%) | 4% (± 0.7%) | Low |

attacks against conventional authentication methods such as fingerprint and PIN-based systems.

The touch-based AHP-RF model demonstrated the highest security score, with only a 3% success rate for mimicry attacks and a 1% success rate for brute-force attacks. Traditional methods like fingerprint and PIN-based systems showed higher vulnerability, confirming the superiority of the proposed approach.

### 4.5. User acceptance and usability testing

The system was also reported to be easy to use, according to the users, and received positive feedback overall. Our exemplary use case showcased that the touch-based authentication enhanced by AHP-driven feature selection was effective and unobtrusive. Overall, the system's usability was rated as easy to use (M = 4.68 on a scale of 1–5).

### 4.6. Discussion

The findings show that AHP, combined with machine learning classifiers, improves authentication performance and security strength. Focusing on the necessary functionalities, the decision-making strength, and the computational complexity of AHP proves potential and trustworthiness in authorizing and authenticating behavior, making the calculation user-friendly. This is another reason for the high resilience of the system against Mimicry and Brute-force attacks, making this method a good alternative to traditional methods.

In summary, the unique idea from this study overcomes those limitations and provides a solution that is both scalable and facilitates secure authentication on smartphones. Future work may forecast further a fusion of AHP with new machine learning structures designed to accommodate dynamic cyber security concerns.

## 5. Conclusion

This paper presents a touch-based user authentication system that combines different machine learning algorithms with the Analytic Hierarchy Process (AHP) for feature selection to achieve high security and reliability compared to existing approaches in smartphone authentication. The logic behind the AHP integration permitted systematic ranking and selection of effective touch and spatial data features, which were then further processed using machine learning classifiers—Random Forest (RF) and Support Vector Machine (SVM)—to enable precise distinction between true users versus potential impostors. Combining these functionalities deals with the weaknesses of traditional authentication methods—PIN codes, passwords, and biometrics by implementing a user-only specific characteristic interaction capability that is difficult to reproduce.

Summary and key findings showed a significant increase in the system's accuracy, where Random Forest achieved an accuracy of 89.7%; also, the FP rate dropped to 4.5%. Attack testing further validated the defense mechanism, indicating a strong resistance to mimicry and brute-force attacks with success rates as low as 1% for brute-force attempts. These results demonstrate the value of integrating AHP with machine learning to build a decision-making layer that improves feature prioritization and model performance, hence both real-time security and efficiency during usage.

The model's accuracy and security were better than conventional authentication methods (fingerprint, PIN, etc.). By directing the classification models on the parts of data that had more impact, AHP-driven feature ranking reduced computational overheads and improved overall model precision with real-time processing feasible. The system's usability was confirmed in user acceptance testing, where participants gave high ratings for ease of use to touch-based authentication, which is probably due to the non-intrusive character of touch-based biometrics.

We present this study as an aid to the emergent area of smartphone-based security systems by proposing a scalable, versatile, and non-intrusive authentication framework when acknowledging the innate and behavioral characteristics of how users touch their devices. A case of AHP in a cyber security context illustrates how decision-making techniques can complement machine learning models and result in systems that are not only efficient but also robust. Future research could explore the potential for expanding this hybrid approach with other machine

learning models, such as deep learning architectures, as well as further field-testing in a wider variety of settings and over a larger, more representative population to evaluate generalization.

In the end, the touch-based authentication model proposed by AHP, with the assistance of touch point features, provides a trustable framework enhancing mobile security, which provides insights to help shape the next generation of mobile authentication systems with robustness and usability. The study results underscore the viability of combining decision-making processes with machine learning towards mobile cyber applications and establishing a new level of performance/quality in balancing security, usability, and real-time delivery.

## Acknowledgement

We sincerely thank the subjects who provided their touch dynamics data for this study.

## Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

## Conflicts of interest

The author declares no conflict of interest.

## Data availability

The data presented in this study are available on request from the authors.

## References

1. A. Pinto *et al.*, "Counteracting presentation attacks in face, fingerprint, and iris recognition," *Deep learning in biometrics*, vol. 245, p. 121, 2018.
2. D. Menotti *et al.*, "Deep representations for iris, face, and fingerprint spoofing detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 864–879, 2015.
3. M. L. Shuwandy, B. B. Zaidan, and A. A. Zaidan, Novel authentication of blowing voiceless password for android smartphones using a microphone sensor Content courtesy of Springer Nature, terms of use apply. Rights reserved. Content courtesy of Springer Nature; terms of use apply. Rights reserved. Multimedia Tools and Applications, 2022.
4. M. L. Shuwandy, B. B. Zaidan, A. A. Zaidan, and A. S. Albahri, "Sensor-based mHealth authentication for real-time remote healthcare monitoring system: A multilayer systematic review," *J Med Syst*, vol. 43, no. 2, 2019, doi: 10.1007/s10916-018-1149-5.
5. B. Zurita, S. Bosque, W. Fuertes, and M. Macas, "Social engineering shoulder surfing attacks (SSAs): A literature review. Lessons, challenges, and future directions," in *Advanced Research in Technologies, Information, Innovation and Sustainability*, T. Guarda, F. Portela, and J. M. Diaz-Nafria, Eds., Cham: Springer Nature Switzerland, 2024, pp. 220–233.
6. K. Wang, L. Zhou, D. Zhang, and J. Lai, "Shoulder surfing on mobile authentication: Perception vis-a-vis performance from the attacker's perspective," in *2023 IEEE International Conference on Intelligence and Security Informatics (ISI), 2023*, pp. 1–6. doi: 10.1109/ISI58743.2023.10297219.
7. M. L. Shuwandy, H. A. Aljubory, N. M. Hammash, M. M. Salih, M. A. Altaha, and Z. T. Alqaisy, "BAWS3TS: Browsing authentication web-based smartphone using 3D touchscreen sensor," *2022 IEEE 18th International Colloquium on Signal Processing and Applications, CSPA 2022 - Proceeding*, no. May, pp. 425–430, 2022, doi 10.1109/CSPA55076.2022.9781888.
8. M. L. Shuwandy *et al.*, "mHealth authentication approach based 3D touchscreen and microphone sensors for real-time remote healthcare monitoring system: Comprehensive review, open issues and methodological aspects," *Comput Sci Rev*, vol. 38, p. 100300, 2020, doi: 10.1016/j.cosrev.2020.100300.
9. A. Y. Younis and M. L. Shuwandy, "Biometric authentication utilizing EEG based-on a smartphone's 3D touchscreen sensor," in *2023 IEEE 14th Control and System Graduate Research Colloquium (ICSGRC)*, IEEE, pp. 169–174, 2023.
10. D. Hassanvand, H. E. Shirvan, M. R. Ghotbi-Ravandi, and M. Beytollahi, "Prioritizing the noise control methods by using the Analytical Hierarchy Process (AHP) method in an Iranian tire factory," *Work*, vol. 70, no. 3, pp. 883–892, 2021.
11. Y. Tian, M. A. Chao, C. Kulkarni, K. Goebel, and O. Fink, "Real-time model calibration with deep reinforcement learning," *Mech Syst Signal Process*, vol. 165, p. 108284, 2022.
12. Y. B. Abushark *et al.*, "Usability evaluation through fuzzy AHP-TOPSIS approach: Security requirement perspective," *Comput. Mater. Contin*, vol. 68, pp. 1203–1218, 2021.
13. M. Wang, X. Yue, C. Gao, and Y. Chen, "Feature selection ensemble for symbolic data classification with AHP," in *2018 24th International Conference on Pattern Recognition (ICPR)*, pp. 868–873, 2018. doi: 10.1109/ICPR.2018.8546098.
14. R. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides, "Biometric authentication on iPhone and Android: Usability, perceptions, and influences on adoption," 2015.
15. C. Braz and J.-M. Robert, "Security and usability: The case of the user authentication methods," in *Proceedings of the 18th Conference on l'Interaction Homme-Machine*, pp. 199–203, 2006.
16. M. L. Shuwandy *et al.*, "Sensor-based authentication in smartphone; A systematic review," *Journal of Engineering Research*, 2024.
17. K. Sathya, J. Esther, S. Kavitha, and J. Kamalakumari, "Facetpass-intelligent facial recognition authentication system security and usability," in *2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)*, IEEE, pp. 1–6, 2024.
18. D. Harikrishnan, N. Sunil Kumar, S. Joseph, and K. K. Nair, "Towards a fast and secure fingerprint authentication system based on a novel encoding scheme," *International Journal of Electrical Engineering & Education*, vol. 61, no. 1, pp. 100–112, 2024.

19. A. Wone, J. Di Manno, C. Charrier, and C. Rosenberger, "Impact of environmental conditions on fingerprint systems performance," in *2021 18th International Conference on Privacy, Security and Trust (PST)*, IEEE, pp. 1–5, 2021.
20. S. Liu, B. Yang, P. C. Yuen, and G. Zhao, "A 3D mask face anti-spoofing database with real-world variations," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pp. 100–106, 2016.
21. A. Eldow, R. A. Alsharida, M. Hammood, M. Shakir, S. I. Malik, A. K. Muttar, and K. A. Kadhim, "Information communication technology infrastructure in sudanese governmental universities," in *Recent Advances in Intelligent Systems and Smart Applications*, pp. 363–375, 2021.
22. C.-A. Toli and B. Preneel, "Provoking security: Spoofing attacks against crypto-biometric systems," in *2015 World Congress on Internet Security (WorldCIS)*, pp. 67–72, 2015, doi: 10.1109/WorldCIS.2015.7359416.
23. M. I. Sharif, M. Mehmood, M. I. Sharif, and M. P. Uddin, "Human gait recognition using deep learning: A comprehensive review," arXiv preprint arXiv:2309.10144, 2023.
24. R. V Yampolskiy and V. Govindaraju, "Behavioural biometrics: A survey and classification," *Int J Biom*, vol. 1, no. 1, pp. 81–113, 2008.
25. B. Pelto, M. Vanamala, and R. Dave, "Your identity is your behavior-continuous user authentication based on machine learning and touch dynamics," in *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, IEEE, pp. 1–6, 2023.
26. P. Aaby, M. V. Giuffrida, W. J. Buchanan, and Z. Tan, "An omnidirectional approach to touch-based continuous authentication," *Comput Secur*, vol. 128, p. 103146, 2023.
27. P. G. do Nascimento, P. Witiak, T. MacCallum, Z. Winterfeldt, and R. Dave, "Your device may know you better than you know yourself–continuous authentication on novel dataset using machine learning," arXiv preprint arXiv:2403.03832, 2024.
28. K. Wang, L. Zhou, and D. Zhang, "Biometrics-based mobile user authentication for the elderly: Accessibility, performance, and method design," *Int J Hum Comput Interact*, vol. 40, no. 9, pp. 2153–2167, 2024.
29. C. Gupta, I. Johri, K. Srinivasan, Y.-C. Hu, S. M. Qaisar, and K.-Y. Huang, "A systematic review on machine learning and deep learning models for electronic information security in mobile networks," *Sensors*, vol. 22, no. 5, p. 2017, 2022.
30. R. A. Disha and S. Waheed, "Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique," *Cybersecurity*, vol. 5, no. 1, p. 1, 2022, doi: 10.1186/s42400-021-00103-8.
31. M. J. De Lucia and A. Srinivasan, "Artificial intelligence and machine learning for network security: Quo vadis?" in *Network Security Empowered by Artificial Intelligence*, Y. Chen, J. Wu, P. Yu, and X. Wang, Eds., Cham: Springer Nature Switzerland, pp. 79–97, 2024. doi: 10.1007/978-3-031-53510-9_3.
32. L. Pryor, J. Mallet, R. Dave, N. Seliya, M. Vanamala, and E. S. Boone, "Evaluation of a user authentication schema using behavioral biometrics and machine learning," arXiv preprint arXiv:2205.08371, 2022.
33. Q. Wang *et al.*, "Exploring the impact of in-browser deep learning inference on quality of user experience and performance," arXiv preprint arXiv:2402.05981, 2024.
34. W. Alhakami, "Evaluating modern intrusion detection methods in the face of Gen V multi-vector attacks with fuzzy AHP-TOPSIS," *PLoS One*, vol. 19, no. 5, p. e0302559, 2024.
35. A. Alharbi *et al.*, "Analyzing the impact of cyber security related attributes for intrusion detection systems," *Sustainability*, vol. 13, no. 22, p. 12337, 2021.
36. C. Goh, J. C. Devlin, D. Deng, A. McDonald, and M. R. Kamarudin, "Uncorrelated weighted median filtering for noise removal in superdarn," in *2014 IEEE 17th International Conference on Computational Science and Engineering*, IEEE, pp. 981–988, 2014.
37. R. Dingliwal, S. Gupta, T. Chopra, and A. Pandey, "Optimization of fractional order low pass filter using a metaheuristic algorithm," in *2022 3rd International Conference for Emerging Technology (INCET)*, pp. 1–6, 2022. doi: 10.1109/INCET54531.2022.9825403.
38. Q. Li, R. Li, K. Ji, and W. Dai, "Kalman filter and its application," in *2015 8th International Conference on Intelligent Networks and Intelligent Systems (ICINIS)*, IEEE, pp. 74–77, 2015.
39. M. Shakir, A. B. Abubakar, Y. Yousoff, M. Al-Emran, and M. Hammood, "Application of confidence range algorithm in recognizing user behavior through EPSB in cloud computing," *Journal of Theoretical and Applied Information Technology*, vol. 94, no. 2, pp. 416–427, 2016.
40. A. Pal and S. Nagarajaiah, "Data fusion based on short-term memory Kalman filtering using intermittent-displacement and acceleration signal with a time-varying bias," *Mech Syst Signal Process*, vol. 216, p. 111482, 2024.
41. M. M. Al-Jarrah, S. S. Al-Khafaji, S. Amin, and X. Feng, "Finger-drawn signature verification on touch devices using statistical anomaly detectors," Proceedings - *2019 IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Internet of People and Smart City Innovation, SmartWorld/UIC/ATC/SCALCOM/IOP/SCI 2019*, no. May, pp. 1700–1705, 2019, doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00303.
42. D. M. Shila and E. Eyisi, "Adversarial gait detection on mobile devices using recurrent neural networks," Proceedings - *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, pp. 316–321, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00055.
43. Y. Liu *et al.*, "Risk factor analysis and establishment of a nomogram model to predict blood loss during total knee arthroplasty," *BMC Musculoskelet Disord*, vol. 25, no. 1, p. 459, 2024.
44. Z. Min *et al.*, "Developing an assessment tool for the healthy lifestyles of the occupational population in China: a modified Delphi-analytic hierarchy process study," *Sci Rep*, vol. 14, no. 1, p. 20359, 2024.
45. T. H. H. Aldhyani and H. Alkahtani, "Artificial intelligence algorithm-based economic denial of sustainability attack detection systems: Cloud computing environments," *Sensors*, vol. 22, no. 13, p. 4685, 2022.
46. M. A. Ahmed, Z. T. Al-Qaysi, M. L. Shuwandy, M. M. Salih, and M. H. Ali, "Automatic COVID-19 pneumonia diagnosis from x-ray lung image: A deep feature and machine learning solution," in *Journal of Physics: Conference Series, IOP Publishing Ltd*, Jul. 2021, doi: 10.1088/1742-6596/1963/1/012099.
47. Z. T. Al-Qaysi *et al.*, "Systematic review of training environments with motor imagery brain-computer interface: Coherent taxonomy, open issues, and recommendation pathway solution," *Health Technol (Berl)*, vol. 11, no. 4, pp. 783–801, 2021, doi: 10.1007/s12553-021-00560-8.

48. D. Supriyadi, S. T. Safitri, and D. Y. Kristiyanto, “Higher education e-Learning usability analysis using system usability scale,” *IJISTECH (International Journal of Information System and Technology)*, vol. 4, no. 1, pp. 436–446, 2020.

49. R. Alsharida, M. Hammood, M. A. Ahmed, B. Thamer, and M. Shakir, “RC4D: A new development of RC4 encryption algorithm," in *Selected Papers from the 12th International Networking Conference: INC 2020*, vol. 12, Springer International Publishing, pp. 19–30, 2021.