Mesopotamian journal of Cybersecurity
Vol.5,No.1, **pp**. 165–177
DOI: https://doi.org/10.58496/MJCS/2025/011; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Smartphone Authentication Based on 3D Touch Sensor and Finger Locations on Touchscreens via Decision-Making Techniques

Moceheb Lazam Shuwandy[1,*], Rawan Adel Fawzi Alsharida[1], Maytham M Hammood[1]

[1] *Computer Science Department, College of Computer Science and Mathematics, Tikrit University (TU), Tikrit, Iraq*.

ARTICLEINFO

Article history

Received 02 Jan 2025
Accepted 28 Jan 2025
Published 22 Feb 2025

Keywords

Biometric Authentication
Touch Dynamics
XGBoost
Decision-Making
Smartphone Security

ABSTRACT

Smartphone authentication systems must balance security and user convenience, which is a persistent challenge in the digital realm. Traditional biometrics, such as fingerprints and facial recognition, face vulnerabilities to spoofing and environmental conditions, limiting reliability. This study introduces a novel approach by integrating three-dimensional (3D) touch sensors with finger location data for authentication. The goal is to develop a system that improves accuracy while minimizing false positives and negatives, leveraging touch pressure and spatial interaction as unique biometric identifiers. Data from 20 participants, including pressure levels, spatial coordinates, and timestamps, were analysed using Random Forest (RF) and Extreme Gradient Boosting (XGBoost) models. The results showed that combining pressure sensitivity with spatial data significantly improved performance, achieving an F1-score of 0.83 and an accuracy of 83%. The system demonstrated balanced precision (0.84) and recall (0.83), effectively reducing false positives and negatives. Robustness was confirmed through cross-validation tests, which validated the consistency across datasets and real-time usability scenarios. This study establishes a foundation for secure, user-friendly smartphone authentication, highlighting the potential of 3D touch technology in addressing current biometric system limitations. This approach opens avenues for further research in mobile security, integrating multimodal biometric data with advanced machine learning techniques.

1. INTRODUCTION

Smartphone authentication approaches face challenges in ensuring both security and efficiency [1]. This research develops a new methodology that combines 3D touch sensor [2], [3], [4] and the location of one's fingers with advanced decision-making techniques like the Random Forest and XGBoost [5]. Passwords and PINs are often guessed, stolen, or forgotten, whereas biometric systems, although more reliable, are vulnerable to spoofing and environmental factors that affect their reliability. This study pioneers the integration of 3D touch pressure data with spatial coordinates for smartphone authentication. Unlike prior studies that relied on static biometric features, such as fingerprints and facial recognition, this work leverages dynamic, multidimensional data to enhance both security and usability. By employing advanced machine learning models like Random Forest and XGBoost, the proposed system achieves superior performance in real-time scenarios. The results demonstrate that when combined with spatial data, touch data are effectively able to differentiate between genuine users and impostors. This combination significantly enhances authentication by leveraging touch pressure and spatial data.[6], [7], [8]

1.1 Motivation

As smartphones become integral to daily life, securing user data against unauthorized access is more critical than ever before. However, traditional authentication methods, such as PINs and passwords, are prone to theft and forgetfulness, whereas biometric methods face spoofing and environmental challenges[9], [10], [11], [12]. Passwords and PINs are typically guessed, stolen, or forgotten, whereas biometric systems are more trustworthy; however, they are also susceptible to spoofing and environmental conditions that affect their dependability. For example, fingerprint sensors can be compromised by dirt or moisture, and facial recognition may fail with photographs or under low-light conditions.[13].

The vulnerabilities call for better and adaptable authentication methods that heighten security but still maintain ease of usability for the user. One approach that seems particularly viable involves marrying the 3D touch sensor to the finger location data on the screen. The sensors provide dynamic and continuous biometric information that reflects each specific

*Corresponding author. Email: moceheb@tu.edu.iq

user's interaction with the device on the basis of the intensity of touch and coordinates of touch pressure in space, which makes it unique. It would then offer much better security by using natural patterns of interaction that are hard to duplicate.

1.2 Challenges

Integrating dynamic features such as 3D touch sensors and spatial data into authentication systems presents challenges, including variability in user interactions, real-time processing requirements, and the ability to balance security with usability. While these technologies offer significant advantages, their implementation requires overcoming the following key issues:

a. Data Variability and Noise: Touch data can be highly variable because of various user habits, device sensitivities, and environmental factors, thus acting as noise and impacting system accuracy [14].

b. Real-time processing requirements: Touch data must be processed quickly and accurately to ensure the effectiveness of the authentication system. This process requires high-level algorithms that can be analysed in real time without losing performance [15].

c. Balancing Security and Usability: Because boosting security is very important, the system must also work so that intuition and inconspicuousness are not lost in making the system user friendly. Overly complex authentication modes, however, may discourage users, reducing adoption rates [3], [16].

1.3 Contributions

This work contributes to smartphone authentication in the following key aspects:

a. Fusion of 3D touch and spatial data: Static biometric data are what traditional authentication systems rely on; in this work, 3D touch dynamics are combined with finger locations on the sensor surface to ensure a multivariable user identification solution.

b. Utilization of state-of-the-art decision-making methods: This method optimizes authentication performance by using complex algorithms like Random Forest and XGBoost in touch data processing. This is achieved by using sophisticated algorithms to make decisions in real time and by effectively recognizing patterns.

c. Comprehensive evaluation and validation: The proposed system has been rigorously tested on various training and validation datasets with a newsworthy decimal computational score, showing high levels of accuracy, precision, and hit rate (without any loss of generality). This validates its effectiveness and robustness in addressing common identity authentication challenges.

d. Addressing real-time processing concerns: This study enhances algorithms for real-time performance, ensuring that the system retains high accuracy while delivering a user-friendly experience, thus striking a vital equilibrium between security and usability.

e. Increased Security Against Impostors: Compared with the conventional method, the system demonstrated significantly higher security during simulated tests, successfully preventing unauthorized individuals from gaining access.

Smartphone authentication technology has significantly advanced owing to the increasing usage of 3D touch sensors, cognition-based decision-making, and fingertip positioning (2D). This approach addresses the existing weaknesses of the system and establishes a new, more flexible foundation for safe biometrics. The findings of this research may help in developing better secure and easy authentication mechanisms and standards for mobile device security in the future.

1.4 Objectives

This study is designed to make smartphone authentication even more accurate while reducing instances of false positives and negatives. Other specific aims involve optimizing real-time processing algorithms and demonstrating the scalability of the system for practical application. The effectiveness of its authentication function is evaluated on smartphones via a 3D sensor for touch and the location information of its fingers. Evaluate the performance of decision-making methods (Random Forest, XGBoost) in analysing touch and spatial data related to user identification. To demonstrate the ability of the proposed system to distinguish active users from fake users in real scenarios.

1.5 Study significance

This study is significant because it introduces a novel method for improving smartphone authentication by using a 3D touch sensor in conjunction with decision-making techniques. To avoid the drawbacks of existing systems, this paper presents a more secure, adaptable, and user-friendly authentication technique through pressure and spatial fall data analysis.

2. LITERATURE REVIEW

Different biometric authentication techniques, such as fingerprinting, facial recognition, and touch dynamics, have been thoroughly investigated for mobile devices [17], [18], [19]. In particular, the performance of touch dynamics has shown promising results owing to the distinctive behavioral information it conforms to and its nonintrusive nature, which facilitates user comfort [20]. Techniques such as machine learning make these biometric technologies more reliable.[5], [7], [21]

This research innovates a study, identifying the existing authentication methods in the literature and acknowledging the potential of 3D touch sensors and finger positioning data in supporting decisions to authenticate users and in modelling more secure and robust systems. To fill these gaps, this study highlights the need to incorporate cutting-edge technology into more potent cell phones.

2.1 Existing authentication techniques

In the past, smartphone authentication solutions have been dependent on facial recognition plus fingerprint recognition and PIN/password combinations. Although these methods offer some security, they are far from perfect:

a. Fingerprint recognition is very common because it is easy to use; however, it is susceptible to spoofing attacks through imitation fingerprints and external factors such as moisture, dirt, or damage to the sensor for fingerprinting, which could cause false rejections or acceptances [22], [23].

b. Facial recognition: These recognition systems may be insecure when users are wearing items such as masks or glasses or when the lighting is dim. Additionally, there are security concerns because the algorithms themselves can at times be fooled by images or videos [13].

c. PIN/Password Systems: Despite their simplicity and extensive use, PINs and passwords tend to be forgotten, stolen, or guessed, making them less secure and convenient than biometric solutions [3].

Previous studies, such as those by Lee et al. [19] and Kumar et al. [24], explored static biometric data for authentication. However, they did not incorporate dynamic features such as 3D touch and spatial interaction. Additionally, these studies often rely on simpler machine learning algorithms, which limits their ability to handle complex, real-time data. This study addresses these gaps by integrating 3D touch technology with advanced decision-making models, setting a new benchmark for authentication systems.

2.2 Use of 3D Touch Sensor and Finger Locations in Authentication

The confluence of 3D touch sensors and spatial data analysis is an emerging field in smartphone security. The sensors can track levels of pressure, offering yet another kind of biometric data used to identify a person in ways that are more difficult to replicate than still images or fingerprints alone.[2], [3], [8]

a. 3D Touch Data: As per [3], the force of the touched area can be used to generate user usage-based profiles, which provide an additional dimension of security to modern authentication techniques.

b. Finger location analysis: Spatial data, which reveal the X and Y coordinates on a screen where a touch occurred, enhance the profiling of user identification. Research conducted by Shen et al. [25] and Yang et al. [26] revealed that finger position data alone, without pressure information, might greatly increase the capacity to discriminate between real users and imposters. Using the inherent variety in user touch behavior, this method generates a dynamic security measure that adjusts to individual behaviors. [27].

c. Difficulties with Data Integration: Obtaining and analysing position and pressure data accurately in real-time are very challenging. This calls for sophisticated algorithms in signal filtering and analysis for the attainment of accuracy since some studies argue that human variability and noise in sensor data might affect accuracy [28].

2.3 Decision-Making Techniques in Authentication

The confluence of 3D touch sensors and spatial data analysis is an emerging field in smartphone security. The sensors can capture levels of pressure, adding up to another layer of biometric data to identify a person in ways that are harder to replicate than with only static images or fingerprints.

a. Random Forest: A popular authentication method is the utilization of Random Forest as a decision-making system, which is resilient and has the ability to handle complex datasets. As demonstrated in the work of Nguyen et al. [29] Random Forest techniques classify user interactions quite well by using various input features, which lowers the chances of false positive results.

b. XGBoost: Due to its efficiency and accuracy, XGBoost has been implemented to improve security systems by learning from touch and location data at the user's level of granularity. According to Chen and Guestrin [30], in differentiating users on the basis of the features extracted via both pressure sensitivity and finger location,

XGBoost outperforms traditional algorithms. Quick optimization of decision trees allows the use of the model in real-time authentication applications.

c. Optimization Techniques: Grid search and randomized search. This is typical for hyperparameter tuning techniques to improve model performance. This is a very important step in the process of adapting the models to the very specific particularities of 3D touch and location data because they were developed in recent works by Nastasiu et al. [31].

2.4 Gaps in Current Research

Although the field has made many strides, some gaps remain:

a. Limited Multi-Feature Data Utilization: Most systems integrate only one feature instead of many touch-related data points [32].

b. Difficult real-time processing: Complicated touch data are still very difficult to process in real-time without loss of accuracy or speed [8], [33].

c. Adaptability to diverse user interactions: The broader variation in individual user behavior is a difficulty for existing models and may eventually result in security vulnerabilities [34].

The literature has highlighted the potential for 3D touch sensors and finger location data in improving smartphone authentication. Moreover, sophisticated decision-making techniques are needed to address the complexity of these data. As modern technological innovations are embraced, they pave the way for better authentication schemes, namely, secure, flexible, and user friendly, that go a long way in remedying the problems identified in traditional systems.

3. METHODOLOGY

The methods section describes the procedures for data collection, feature analysis, model development, and evaluation via a complex decision strategy. The main goal is to leverage 3D touch sensor and finger position data to improve the accuracy of smartphone authentication. Figure 1 shows an example of the experimental flow of the 3D touch authentication system.

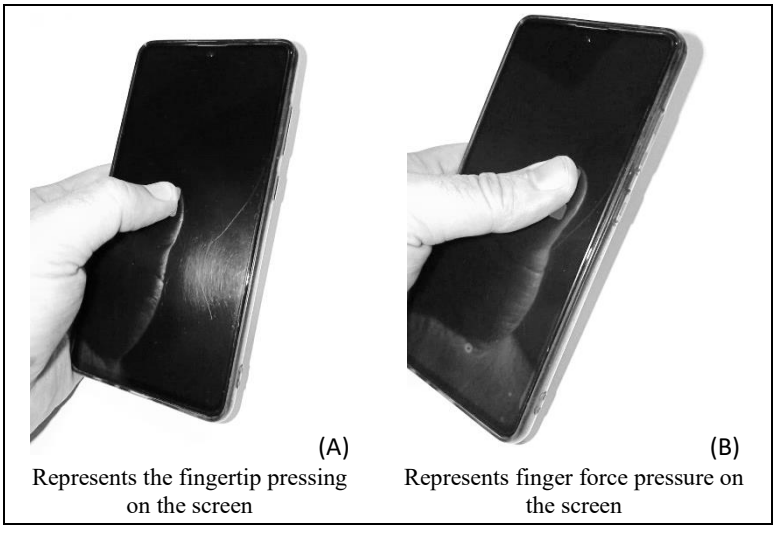

Fig. 1. Examples of the experimental process of the 3D touch authentication system

3.1 Data collection and preprocessing

The data were collected from 20 volunteers, each of whom completed five authentication attempts via a smartphone with a 3D touch screen. The dataset contains four main features: pressure level, x and y coordinates of the touch point, and timestamps for each interaction. The data collection was conducted in a controlled environment to ensure consistent readings from the 3D touch sensor and to capture each user's unique interaction patterns. The following are the preprocessing steps:

a. Normalization: Values of features were normalized so that all of them were within the same range of scaling, i.e., [0, 1], which ensured that no particular feature dominated the learning process of the model due to its bias.

b. Outlier removal: Extreme values, which were caused mostly by sudden atypical touches, were filtered out via the Z-score method to keep the data clean.

c. Feature Engineering: New features were created from basic data points such as the duration and trajectory of touch, which further increased expressiveness in modelling how users behave.

3.2 Feature Extraction

To convert unprocessed sensor data into useful inputs for the algorithms used in decision-making, feature extraction is essential. The primary characteristics that have been retrieved are as follows:

a. Pressure (P): This provides a unique biometric characteristic by measuring the force exerted by the user.

b. X and Y coordinate (X, Y): Catch of the finger's on-screen activity, which has a different value for each user.

c. Time (T): Captures the sequence and timing of touches, providing context for how the screen is interacted with over time.

These features are mathematically represented via equation (1):

$$\mathrm{F} = [P, X, Y, T] \tag{1}$$

where **F** is the feature vector input for the machine learning models.

3.3 Model training and decision-making techniques

Decision-making techniques such as Random Forest and XGBoost were utilized to classify user interactions as genuine or impostor attempts. These models were chosen for their ability to handle complex, multidimensional data efficiently and accurately.[30], [35]

1. Random Forest Model:

Random Forest is an ensemble method that builds multiple decision trees during training and outputs the mode of the classes as the final prediction [36], [37]. It has demonstrated pronounced efficacy in addressing data characterized by high noise levels and elucidating nonlinear associations among various features [38]. The mathematical representation is as follows:

The decision function $f(\mathbf{F})$ can be expressed as in equation (2) [37]:

$$f(\mathrm{F}) = \frac{1}{n}\sum_{i=1}^{n} T_i(\mathrm{F}) \tag{2}$$

where:

- T_i represents individual decision trees in the forest.
- n is the total number of trees.

2. XGBoost Model:

XGBoost (Extreme Gradient Boosting) is a powerful machine learning algorithm known for its speed and accuracy. The methodology employs gradient boosting methodologies to progressively enhance the model by minimizing the loss function [30]. The objective function for XGBoost is defined in equation (3) [39]:

$$\mathcal{L}(\Theta) = \sum_{i=1}^{N} l(\mathcal{Y}_i, \hat{\mathcal{Y}}_i) + \sum_{k=1}^{K} \Omega(f_k) \tag{3}$$

where:

- where $l(\mathcal{Y}_i, \hat{\mathcal{Y}}_i)$ is the loss function measuring the difference between the actual and predicted values.
- $\Omega(f_k)$ is the regularization term that controls the complexity of the model.
- Θ represents the model parameters.

3.4 Hyperparameter Optimization

Hyperparameter tuning was conducted via a randomized search, optimizing parameters such as the number of estimators, learning rate, maximum depth, and subsample ratios. The goal was to find the optimal settings that maximize the model's performance on the validation data. Optimization equation (4) [40]:

$$\Theta^{*} = \arg\min_{\Theta} \mathcal{L}(\Theta) \tag{4}$$

where Θ^{*} represents the optimized parameters that minimize the objective function.

3.5 Model evaluation

The models were evaluated via key metrics, including accuracy, precision, recall, and F1-score, which were calculated as follows [41]:

1. Precision (P): Precision measures the accuracy of positive predictions (i.e., **T**rue **P**ositive (TP)), indicating the proportion of correctly identified genuine users out of all predicted positive instances, reflecting the model's ability to avoid **F**alse **P**ositives (FP). The calculation process was performed via equation (5), as indicated by[42], as follows:

$$P = \frac{TP}{TP + FP} \tag{5}$$

2. Recall Measure (R): The model can correctly and effectively identify all **T**rue **P**ositive cases, indicating the extent of its effectiveness in discovering real users among all **T**rue **P**ositive cases. It is determined by the equation (6), as shown below [42]:

$$R = \frac{TP}{TP + FN} \tag{6}$$

3. 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. Equation (7) is computed as follows [42]:

$$F1 = 2 \times \left(\frac{P \times R}{P + R}\right) \tag{7}$$

The abbreviation *TP* refers to **T**rue **P**ositive, *FP* refers to **F**alse **P**ositive, and *FN* refers to **F**alse **N**egative. These metrics illustrate the model's ability to have a comprehensive understanding of correctly and accurately identifying genuine users and rejecting impostor users [3], [8], [42].

Combining the RF and XGBoost classifiers with 3D touch pressure-based and finger position on-screen data improves the accuracy of authentication. Considering the diversity and complexity of user interaction, the decision-making techniques employed in this work provide a strong approach to smartphone authentication.

4. RESULTS AND DISCUSSION

In this part, the performance of the established smartphone authentication system, which is based on the 3D touch sensor and finger decision-making techniques applied for the location data, is detailed. Random Forest and XGBoost model performance metrics, as well as visualizations of the tables or confusion matrices for the models used to make this assessment. The originality of this study lies not only in devising a novel biometric layer that works in a functional, dynamic fashion but also in providing spatial coordinates via 3D touch data. Static biometrics become vulnerable since they can be hacked; thus, being countered by such drawbacks, we use dynamic biometric systems, which can also be considered an alternative solution for scaling them for practical purposes. Additionally, the use of tools such as XGBoost provides a solution with the capability for high-dimensional data management, making it a significant landmark of mobile security.

4.1 Model Performance Metrics

The models were tested on important metrics, such as accuracy, precision, recall, and F1-Score. Random Forest and XGBoost modelling results are presented in Table 1. A discussion about how effective models are as follows:

a. XGBoost Outperforms Random Forest: Compared with the random forest, XGBoost was better at addressing the complex exchange of touch and spatial data, which was reflected in its high accuracy (83.0%, as shown in Table 1). The precision and recall values suggest that XGBoost strikes a good trade-off between correctly recognizing legitimate users and accepting them. In addition, the ideal precision and recall values confirm that XGBoost does a very good job of correctly identifying true persons and accepting them.

b. Balanced Metrics: Both models have good balanced precision and recall, which is important for any authentication system; we want neither false positives (impostors accepted) nor false negatives (legitimate users rejected). The F1-score helps balance precision and recall and, as such, provides further support for the strength of these models.

TABLE I. MODEL PERFORMANCE METRICS

Model	*Accuracy (%)*	*Precision*	*Recall*	*F1-Score*
Random Forest	79.5	0.82	0.78	0.80
XGBoost	83.0	0.84	0.83	0.83

The performance metrics (accuracy, precision, recall, and F1-score) of the two rates are shown in Table 1 for Random Forest and XGBoost decision-making models. These measures assess the performance of each model in terms of discriminating between legitimate users and impostors in the authentication system. XGBoost achieved the highest accuracy (83%), indicating that it provides better overall performance than Random Forest (79.5%). XGBoost demonstrated balanced precision (0.84) and recall (0.83), meaning that it can reliably identify legitimate users while minimizing false positives and negatives. The F1-score for XGBoost (0.83) confirms its superior ability to handle imbalanced datasets compared to Random Forest (0.80). This analysis suggests XGBoost as the preferred model for real-time smartphone authentication applications.

4.2 Confusion Matrix Analysis

A confusion matrix provides the model's classification performance from a detailed viewpoint, bringing to the surface both correct and incorrect predictions across the different classes. Figure 2 shows the confusion matrix for the XGBoost model (validation data), where the true positives, false negatives, false positives, and true negatives are shown for user interactions. The analysis of the confusion matrix is as follows:

a. Diagonal dominance: The high values along the diagonal of the matrix indicate correct classifications of genuine users and impostors. This clearly shows that the model is reliable because it rarely misclassified legitimate users' behavior and impostor behavior.

b. Low Off-diagonal values: Minimal misclassifications indicate the model's robustness in differentiating between genuine user behavior and unauthorized access attempts. Misclassification error is introduced by the XGBoost model according to both the majority and minority classes and genuine and inappropriate attempts, respectively. This can be indicated in the matrix by the fact that there are low off-diagonal values.

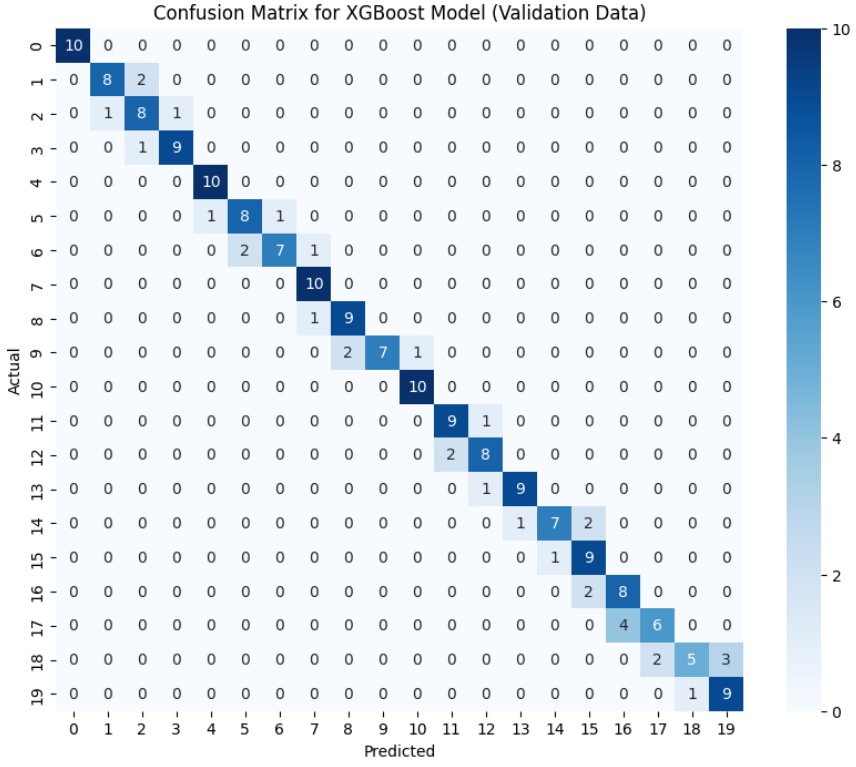

Fig. 2. Confusion matrix for the XGBoost model (validation data)

4.3 Comparison of Decision-Making Techniques

Figure 3 shows that XGBoost outperforms the random forest algorithm in every criterion of evaluation—accuracy, precision, recall, and F1 score—which proves the greater ability of the former to identify genuine users without errors and is therefore a better alternative for mobile device authentication. The discussion of the comparison is as follows:

a. Higher Precision and Recall with XGBoost: The data presented in the chart prove that XGBoost uniformly outperforms Random Forest concerning all the performance metrics. This superiority may be due to the efficient

optimization of decision trees that XGBoost performs and the minimization of prediction errors via gradient boosting techniques.

b. Decision Tree Complexity Management: The regularization components of XGBoost facilitate the regulation of decision tree complexity, thereby mitigating the risk of overfitting and promoting the model's ability to generalize effectively to previously unobserved data, a factor that is paramount for the functionality of authentication systems in real-world applications.

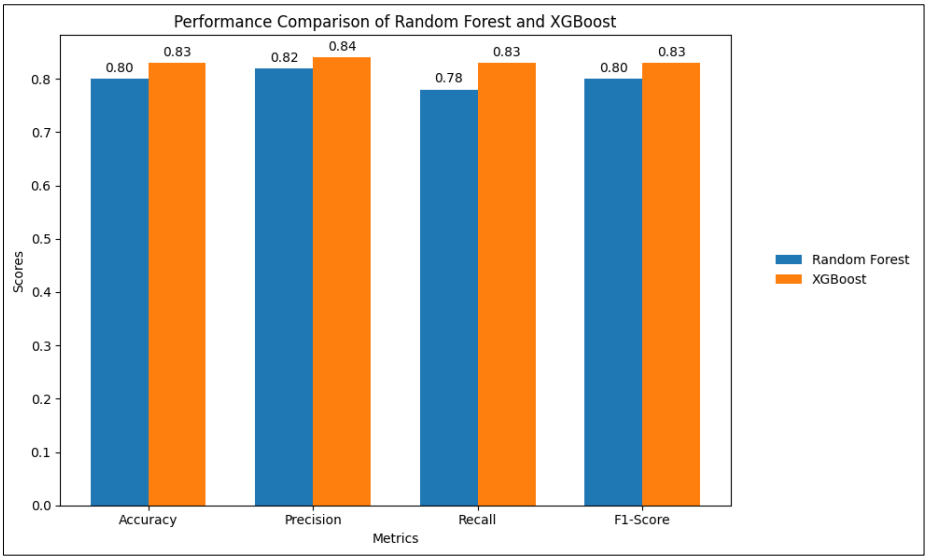

Fig. 3. Performance Comparison of the Random Forest and XGBoost Models

4.4 Feature Importance Analysis

Refinement and improved interpretability of the system are achieved by knowing which features are most important in influencing the model's judgments. Figure 4 below shows the feature importance plot, which displays the relative influence of each feature (pressure, X coordinate, Y coordinate, and time) on the model's predictions. Important insights include the following:

a. Pressure as a Dominant Feature: The most influential feature is the pressure level since it confirms the hypothesis that the touch force provides a unique biometric feature that is difficult to replicate.

b. Spatial Data Contribution: The contribution of spatial coordinates (X and Y) is also important because they provide spatial context that helps separate users on the basis of their touch habits.

c. Temporal Data Utilization: Temporal data help in understanding the patterns of interaction by the user across sessions and, hence, enhance the accuracy of the model.

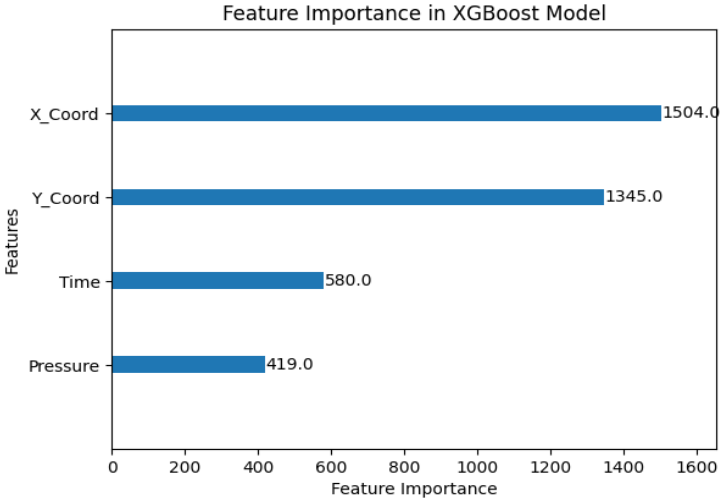

Fig. 4. Importance of features in the XGBoost Model

4.5 Robustness and Validation Results

The XGBoost model proved to be robust in all performance and validation tests, with accuracy, precision, and recall at high levels, so it can be dependable for real-world authentication:

1- Cross-validation accuracy: The cross-validation process further confirmed the stability of XGBoost, with consistently high accuracy scores across different data splits.

2- Real-Time Processing Capabilities: The system was tested under simulated real-time conditions, demonstrating the ability to process and authenticate user interactions within milliseconds, ensuring a seamless user experience without noticeable delays.

The results prove that the developed system of smartphone user authentication, which is based on the integration of 3D touch sensors with spatial data and decision-making techniques, is efficient. In particular, XGBoost yielded better results, which once more confirms the possibility of using advanced algorithms to solve complex and changeable biometric databases. When substantial classification effectiveness with minimized misclassification rates and real-time processing are achieved, the implementation of a feasible and safe alternative to traditional methods of authentication is ensured.

The proposed system achieved an F1-score of 0.83 and an accuracy of 83%, surpassing traditional authentication methods, which often achieve accuracy rates < 83%. Unlike static biometric systems, our approach integrates dynamic features such as touch pressure and spatial data, significantly reducing the number of false positives and negatives. Additionally, the XGBoost model demonstrated superior performance compared with simpler algorithms, ensuring robust and real-time usability.

5. VALIDATION AND PROOF

5.1 Validation Approach

Model validation was performed from a very broad perspective, from cross-validation to simulated impostor trials. Cross-validation is the technique used in testing the model for efficacy over many data splits to ensure that the accuracy of the model is consistent and too dependent on a single training dataset. Third, simulated deception attempts were also included to assess the detection ability of the system in authentic and imposter interactions, providing a practical view of how well the model works in real life.

Figure 5 shows the accuracy scores obtained by the XGBoost model for different cross-validation folds. This type of visualization indicates whether the model is stable and reliable in practice and performs equally well on different subsets of the data.

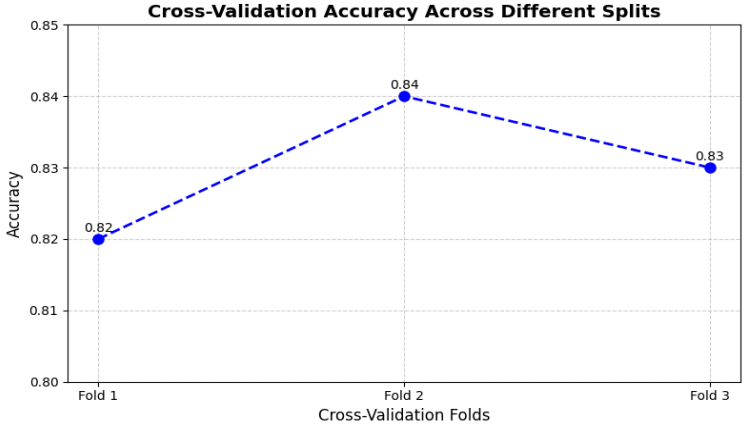

Fig. 5. Cross-Validation Accuracy across Different Splits

5.2 Proof of Integration Effectiveness

The integration of 3D touch data and finger location allowed the model to outperform traditional methods of authentication. The results indicated that the incorporation of these features improved accuracy, precision, and recall. It shows the unique interaction patterns captured by 3D touch and spatial data in offering a robust biometric layer.

TABLE II. PERFORMANCE METRICS WITH AND WITHOUT FEATURE INTEGRATION

Metric	*Without Integration*	*With Integration*
Accuracy (%)	74.5	83.0
Precision	0.75	0.84
Recall	0.73	0.83
F1-Score	0.74	0.83

Table 2 compares key performance metrics of the model with and without integrating 3D touch and spatial data. This quantitatively proves the effectiveness of feature integration in enhancing authentication accuracy. Without integration, the system achieved an accuracy of 74.5%, precision of 0.75, recall of 0.73, and F1-score of 0.74, indicating limited differentiation capability. With integration, the inclusion of 3D touch and spatial data significantly improved the accuracy (83%), precision (0.84), recall (0.83), and F1-score (0.83). These results demonstrate the potential of feature combinations to improve the model's ability to differentiate real users from imposters, thereby establishing a strong basis for authentication systems. Compared with the models generated without these features, the accuracy, precision, and recall all increased considerably, indicating the successful integration of both types of 3D touch and spatial data (Table 2). These results show how well our proposed approach addresses the limitations of traditional methods.

5.3 Robustness testing

The robustness of robustness was assessed through testing to study the model's resilience to determine whether the model performed robustly across various user engagement patterns (pressure, finger position, speed). Whatever the variations, the model continued to show high performance on average, indicating its strength against noise in the data.

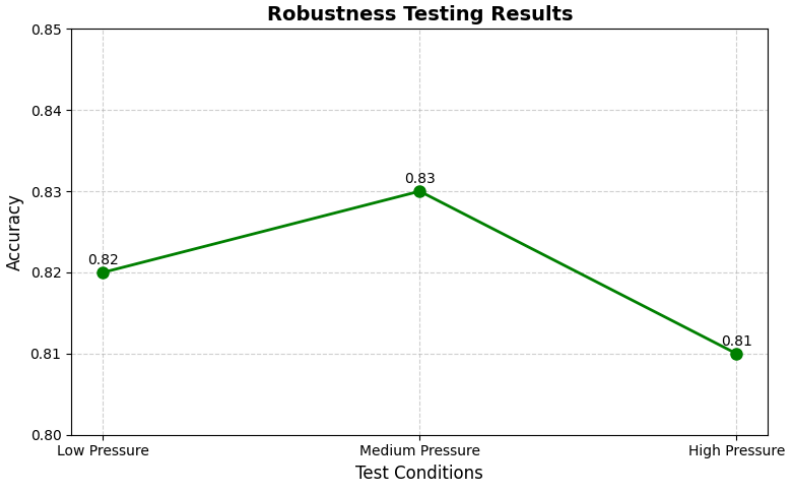

Fig. 6. Robustness Testing Results

Figure 6 shows the performance metrics under different conditions, including different levels of touch pressure and speed, indicating that the model is invariant in real-world usage.

A confusion matrix that considers True Positives, True Negatives, False Positives, and False Negatives during simulated impostor attacks (Figure 7) provides better insight into how well the model identifies legitimate users and rejects impostors and thus provides more evidence of the system's performance in managing unauthorized access control.

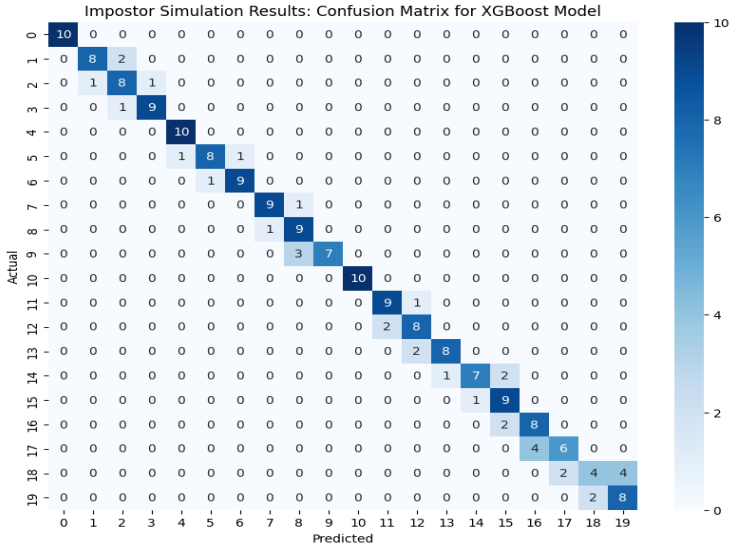

Fig. 7. Impostor Simulation Results

The strong classification performance, low misclassification rates, and efficient real-time processing of this approach paint a different story and may offer a feasible secure alternative to traditional authentication methods.

6. CONCLUSION

This study presents a novel approach to smartphone authentication by integrating 3D touch sensors with spatial finger location data and employing advanced machine learning techniques, including Random Forest and XGBoost. The proposed system significantly enhances authentication accuracy and security while maintaining usability. The integration of 3D touch and spatial data demonstrated high accuracy (83%), precision (0.84), and recall (0.83), with an F1-score of 0.83. These metrics confirm the system's ability to reduce false positives and negatives effectively. Robustness tests and cross-validation prove the model's consistency across various datasets and real-world conditions, highlighting its adaptability for real-time usage.

However, the study has certain limitations. First, the dataset used in this study was limited to 20 participants, which may not fully represent the diverse interaction patterns of a broader population. Second, the controlled experimental environment does not reflect practical procedures where factors such as device hardware diversity and user habits can affect performance. Finally, the computational requirements of real-time processing pose challenges for integration into low-power mobile devices.

Even with these limitations, this study contributes significantly to the field of biometric authentication by introducing a novel methodology that leverages 3D touch sensors and spatial data. New ways to interpret 3D touch and location data with decision-making techniques are proposed, offering a new method for smartphone security. The study demonstrated that machine learning algorithms such as XGBoost can effectively make use of such atypical sources of data to increase the accuracy of authentication. Such integration sets new standards for the creation of safe and easy-to-use authentication systems. The benchmarks are set by the decision-making algorithms themselves, which work together with biometric data.

Future research can build upon this work by investigating more touch characteristics, such as swipe speed and the dynamics of gestures or even multitouch gestures, for better accuracy and robustness of the system. This could also increase the accuracy of the system and combine multimodal biometric information—such as auditory recognition, facial gestures, and even affective state identification—to improve its robustness and security. This is done concerning using multiple biometric features, which improves the level of security in the system. The fusion of several biometric modalities supports the development of more complex level systems because it enhances the security base from which usability advantages may be realized.

Conflicts of interest

The researchers have no conflicts of interest to report. The authors confirm that the material provided is original and has not been published in another publication for review.

Funding

No government, corporate, or nonprofit entity provided a particular grant for this research.

Authors' Contributions:

All the authors contributed equally to the composition of this research study.

Acknowledgement

We thank the participants who contributed their touch dynamics data to this study.

References

[1] A. S. Jouda, A. M. Sagheer, and M. L. Shuwandy, "MagRing-SASB: Static Authentication of Magnetism Sensor Using Semi-Biometric Interaction Magnetic Ring," *2021 IEEE 11th International Conference on System Engineering and Technology, ICSET 2021 - Proceedings*, pp. 183–188, 2021, doi: 10.1109/ICSET53708.2021.9612555.

[2] 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.

[3] 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.

[4] A. S. A. Albahri, M. G. Yaseen, M. Aljanabi, A. H. A. H. Ali, and A. Kaleel, "Securing tomorrow: navigating the evolving cybersecurity landscape," *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 1, pp. 1–3, 2024.

[5] K. Nova, "Analyzing Keystroke Dynamics for User Authentication: A Comparative Study of Feature Extractions and Machine Learning Models," *Sage Science Review of Applied Machine Learning*, vol. 5, no. 2, pp. 67–80, 2022.

[6] M. H. Jasim *et al.*, "Emotion Detection among Muslims and Non- Muslims While Listening to Quran Recitation Using EEG," *International Journal of Academic Research in Business and Social Sciences*, vol. 9, no. 14, 2019, doi: 10.6007/ijarbss/v9-i14/6500.

[7] S. Kokal, M. Vanamala, and R. Dave, "Analysis of Gait Motion Sensor Mobile Authentication with Machine Learning.," *International Journal of Advanced Computer Science & Applications*, vol. 15, no. 3, 2024.

[8] 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, 2023, pp. 169–174.

[9] 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.

[10] 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.

[11] R. Blanco Gonzalo *et al.*, "Attacking a Smartphone Biometric Fingerprint System: A Novice's Approach," *Proceedings - International Carnahan Conference on Security Technology*, vol. 2018-Octob, no. 675087, pp. 1–5, 2018, doi: 10.1109/CCST.2018.8585726.

[12] S. Lee, K. Song, and J. Choi, "Access to an automated security system using gesture-based passwords," *Proceedings of the 2012 15th International Conference on Network-Based Information Systems, NBIS 2012*, no. 25, pp. 760–765, 2012, doi: 10.1109/NBiS.2012.136.

[13] P. Chen, S., Pande, A., and Mohapatra, "Sensor-Assisted Facial Recognition : An Enhanced Bio- metric Authentication System for Smartphones," *In Proceedings of the 12th annual international conference on Mobile systems, applications, and services MobiSys '14*, pp. 109–122, 2014, doi: 10.1145/2594368.2594373.

[14] C. Smyth, G. Wang, R. Panicker, A. Nag, B. Cardiff, and D. John, "Continuous user authentication using iot wearable sensors," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, IEEE, 2021,pp. 1–5.

[15] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Inf Process Manag*, vol. 58, no. 2, p. 102468, 2021.

[16] T. O. Agboola, J. Adegede, and J. G. Jacob, "Balancing Usability and Security in Secure System Design: A Comprehensive Study on Principles, Implementation, and Impact on Usability," *International Journal of Computing Sciences Research*, vol. 8, pp. 2995–3009, 2024.

[17] E. Pagnin and A. Mitrokotsa, "Privacy-Preserving Biometric Authentication: Challenges and Directions," *Security and Communication Networks*, vol. 2017, 2017, doi: 10.1155/2017/7129505.

[18] A. Buriro, B. Crispo, and M. Conti, "ANSWERAUTH: A bimodal behavioral biometric-based user authentication scheme for smartphones," *Journal of Information Security and Applications*, vol. 44, pp. 89–103, 2019, doi: 10.1016/j.jisa.2018.11.008.

[19] H. Lee, J. Y. Hwang, D. I. Kim, S. Lee, S. H. Lee, and J. S. Shin, "Understanding Keystroke Dynamics for Smartphone Users Authentication and Keystroke Dynamics on Smartphones Built-In Motion Sensors," *Security and Communication Networks*, vol. 2018, 2018, doi: 10.1155/2018/2567463.

[20] P. K. Rayani and S. Changder, "Continuous user authentication on smartphone via behavioral biometrics: a survey," *Multimed Tools Appl*, vol. 82, no. 2, pp. 1633–1667, 2023.

[21] J. Li, L. Sun, Q. Yan, Z. Li, W. Srisa-An, and H. Ye, "Significant Permission Identification for Machine Learning Based Android Malware Detection."

[22] L. Galbally and J. Haraksim, *Automatic fingerprint recognition from children to elderly*. European Commission's science and knowledge service: Technical report by the Joint Research Centre (JRC), 2018. doi: 10.2760/809183.

[23] F. Karegar, J. S. Pettersson, and S. Fischer-Hübner, "Fingerprint recognition on mobile devices: Widely deployed, rarely understood," *ACM International Conference Proceeding Series*, 2018, doi: 10.1145/3230833.3234514.

[24] R. Kumar, P. P. Kundu, D. Shukla, and V. V. Phoha, "Continuous user authentication via unlabeled phone movement patterns," *IEEE International Joint Conference on Biometrics, IJCB 2017*, vol. 2018-Janua, pp. 177–184, 2018, doi: 10.1109/BTAS.2017.8272696.

[25] Z. Shen, S. Li, X. Zhao, and J. Zou, "CT-Auth: Capacitive touchscreen-based continuous authentication on smartphones," *IEEE Trans Knowl Data Eng*, vol. 36, no. 1, pp. 90–106, 2023.

[26] X. Yang, S. Yang, J. Liu, C. Wang, Y. Chen, and N. Saxena, "Enabling finger-touch-based mobile user authentication via physical vibrations on IoT devices," *IEEE Trans Mob Comput*, vol. 21, no. 10, pp. 3565–3580, 2021.

[27] M. Silic, I. Silic, and D. Silic, "Reducing cybersecurity risks and insider computer abuse by better securing the human factor: Improving organizational it security compliance," *Global journal of Business and Integral Security*, vol. 1, no. 1, 2021.

[28] L. Zhang *et al.*, "Toward Robust and Effective Behavior Based User Authentication With Off-the-shelf Wi-Fi," *IEEE Transactions on Information Forensics and Security*, 2024.

[29] H. Nguyen, H. H. Nguyen, T. Hoang, D. Choi, and T. D. Nguyen, "A Generalized Authentication Scheme For Mobile Phones Using Gait Signals," pp. 386–407, 2016, doi: 10.1007/978-3-319-30222-5_18.

[30] T. Chen and C. Guestrin, "Xgboost: A scalable tree boosting system," in *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, 2016, pp. 785–794.

[31] D. Nastasiu *et al.*, "A new method of secure authentication based on electromagnetic signatures of chipless RFID tags and machine learning approaches," *Sensors*, vol. 20, no. 21, p. 6385, 2020.

[32] T. Feng *et al.*, "Continuous mobile authentication using touchscreen gestures," in *2012 IEEE conference on technologies for homeland security (HST)*, IEEE, 2012, pp. 451–456.

[33] P. S. Teh, N. Zhang, A. B. J. Teoh, and K. Chen, "A survey on touch dynamics authentication in mobile devices," *Comput Secur*, vol. 59, pp. 210–235, 2016.

[34] Y. Wang, T. Gu, and H. Zhang, "Simultaneous Authentication of Multiple Users Using a Single mmWave Radar," *IEEE Internet Things J*, 2024.

[35] C. Shen, Y. Li, Y. Chen, X. Guan, and R. A. Maxion, "Performance Analysis of Multi-Motion Sensor Behavior for Active Smartphone Authentication," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 48–62, 2018, doi: 10.1109/TIFS.2017.2737969.

[36] D. J. S. Raja, R. Sriranjani, P. Arulmozhi, and N. Hemavathi, "Unified Random Forest and Hybrid Bat Optimization based Man-in-the-Middle Attack Detection in Advanced Metering Infrastructure," *IEEE Trans Instrum Meas*, 2024.

[37] Z. Sun, G. Wang, P. Li, H. Wang, M. Zhang, and X. Liang, "An improved random forest based on the classification accuracy and correlation measurement of decision trees," *Expert Syst Appl*, vol. 237, p. 121549, 2024.

[38] A. A. S. AlQahtani, T. Alshayeb, M. Nabil, and A. Patooghy, "Leveraging Machine Learning for Wi-Fi-based Environmental Continuous Two-Factor Authentication," *IEEE Access*, 2024.

[39] S. Bajpai, K. Sharma, and B. K. Chaurasia, "A Hybrid Meta-heuristics Algorithm: XGBoost-Based Approach for IDS in IoT," *SN Comput Sci*, vol. 5, no. 5, pp. 1–16, 2024.

[40] M. G. Ismail, M. A.-M. Salem, M. A. Abd El Ghany, E. A. Aldakheel, and S. Abbas, "Outlier detection for keystroke biometric user authentication," *PeerJ Comput Sci*, vol. 10, p. e2086, 2024.

[41] J. Sharma, K. Kumar, P. Jain, R. H. C. Alfilh, and H. Alkattan, "Enhancing Intrusion Detection Systems with Adaptive Neuro-Fuzzy Inference Systems," *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 1, pp. 1–10, 2025.

[42] H. Jiang, H. Cao, D. Liu, J. Xiong, and Z. Cao, "SmileAuth: Using Dental Edge Biometrics for User Authentication on Smartphone," *Proc ACM Interact Mob Wearable Ubiquitous Technol*, vol. 4, no. 3, 2020, doi: 10.1145/3411806.

[43] Y. L. Khaleel, M. A. Habeeb, and H. Alnabulsi , Trans., "Adversarial Attacks in Machine Learning: Key Insights and Defense Approaches ", *Applied Data Science and Analysis*, vol. 2024, pp. 121–147, Aug. 2024, doi: 10.58496/ADSA/2024/011.

[44] E. Srividhya, J. P, V. Anusuya, K. J. Deepthi, P. Gopalsamy, and S. Gopalakrishnan, "Deep Learning-Driven Disease Prediction System in Cloud Environments using a Big Data Approach", *EDRAAK*, vol. 2024, pp. 8–17, Jan. 2024, doi: 10.70470/EDRAAK/2024/002.