Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Enhancing Online Child Safety through Age Detection Using Behavioral Interaction Patterns

Nourah Al-humaid[1]✉ and Sulaiman Al Amro[2]
[1]Department of Computer Science College of Computer Qassim University Buraydah 52389, Saudi Arabia
(e-mail: nourahalhumaid.12@gmail.com)
[2]Department of Computer Science College of Computer Qassim University Buraydah 51452, Saudi Arabia
(e-mail: samro@qu.edu.sa)
Corresponding Author: Sulaiman Al Amro **E-mail**: *samro@qu.edu.sa*

| ABSTRACT
This study proposes an intelligent model for accurately distinguishing between children and adults based on diverse behavioral biometrics collected from touchscreen interactions. As digital platforms become increasingly widespread, the demand for effective and privacy-preserving user classification methods has grown—particularly in the context of child online protection. Behavioral features such as touch pressure, swipe velocity, gesture angle, touch frequency, distance, and timing were extracted as participants interacted with a custom-designed mobile game. The dataset included 200 real-world participants (98 children and 102 adults), and two machine learning models were employed: a Convolutional Neural Network (CNN) and a Bagging ensemble classifier. Experimental results demonstrated that both models achieved excellent performance, with the Bagging model attaining an accuracy of 99.3% and the CNN achieving 98.82%. The superior accuracy is attributed to the rich and varied set of behavioral features, which enabled the models to capture subtle differences between age groups effectively. These findings confirm the feasibility of using touch-based interaction data for age-group classification and offer a practical, non-invasive solution for enhancing child safety in digital environments. The proposed framework can be integrated into mobile applications to provide real-time age verification, particularly on platforms offering sensitive content. Moreover, the approach safeguards user privacy by eliminating the need for personally identifiable information, cameras, or microphones.

| KEYWORDS

behavioral biometrics; touchscreen interaction; intelligent model; convolutional neural network (CNN); bagging algorithm; child online protection.

| ARTICLE INFORMATION

ACCEPTED: 03 October 2025 **PUBLISHED:** 17 October 2025 **DOI:** 10.32996/jcsts.2025.7.10.34

1. Introduction

In the era of accelerating digital transformation, the Internet has become an integral part of daily life for individuals of all ages, including children. The widespread accessibility of smart devices has led to a significant increase in children's presence on online platforms, whether for educational, recreational, or social purposes. However, this growing digital engagement raises serious concerns about children's safety online, as they may be exposed to inappropriate content, harmful interactions, or even cyberbullying.

Many digital platforms rely on traditional age verification methods, such as requesting personal information or using knowledge-based questions. Unfortunately, these methods are often ineffective, as children can easily bypass them [1]. Therefore, there is a pressing need for innovative and reliable techniques to accurately detect children's presence online while preserving user privacy.

Behavioral biometrics has emerged as a promising alternative. This approach analyzes users' behavioral patterns during device interaction—such as touch pressure, swipe speed, gesture angles, and timing—to differentiate between children and adults.

Unlike conventional methods, behavioral biometrics operates passively in the background and does not require sensitive personal data, cameras, or microphones, thus offering a more ethical and privacy-conscious solution.

Studies have shown that children exhibit distinct interaction patterns compared to adults. For example, children tend to apply different levels of pressure, display less consistent swipe behavior, and exhibit irregular timing during screen interactions [2]. These differences can be leveraged to develop intelligent systems capable of classifying users by age group, enabling online platforms to tailor content appropriately and implement safety measures in real time.

Despite the technical challenges associated with accurately collecting and analyzing behavioral data, advancements in machine learning and artificial intelligence have significantly improved the effectiveness of such systems. Moreover, behavioral biometrics is difficult to manipulate, making it a sustainable and secure approach for user identification.

This research aims to explore the feasibility and effectiveness of behavioral biometrics in identifying child users on online platforms. It addresses gaps in the current literature by incorporating behavioral features into machine learning models and evaluating their performance. Ultimately, this work contributes to the development of safer and more ethical methods for online age estimation, supporting the broader goal of protecting children in digital environments.

The extensive variety of behavioral features extracted from touchscreen interactions—including touch pressure, swipe velocity, gesture angles, touch frequency, spatial distances, and timing—significantly contributed to the high accuracy achieved by our models. This comprehensive feature set enables capturing subtle behavioral distinctions between children and adults that simpler models might overlook. The following sections of this paper are organized as follows: Section 2 reviews relevant background and related work in behavioral biometrics and age classification; Section 3 describes the proposed methodology, including data collection and feature extraction; Section 4 presents experimental results and evaluation; Section 5 discusses the findings in the context of existing literature; and Section 6 concludes the study and outlines future research directions

2. Background

With the increasing prevalence of digital technology and its penetration into various aspects of daily life, determining the age groups of users on electronic platforms has become an increasingly important issue, especially with the growing use of the Internet by children. Research shows that traditional methods of determining ages, such as data entry forms or identity verification, suffer from significant problems related to their accuracy and ease of bypassing. In this context, behavioral biometrics has emerged as an innovative and more specialized approach, based on studying and analyzing the behavioral interaction patterns of users with digital devices.

Behavioral biometrics is based on extracting unique characteristics from users' interactions with screens, such as click duration, screen pressure, distance between touches, reaction speed, and swipe or vertical swipe angle. Studies show that children, due to their age and cognitive nature, show clear differences in these behavioral patterns compared to adults. For example, children typically show fluctuating reaction speeds, inconsistent screen pressures, and shorter and more random touch distances compared to adults, who are characterized by more regular and stable interaction patterns [2].

The specialization of this technology lies in its ability to operate in real-world environments without the need to obtain sensitive personal data, making it an ideal choice for online child protection applications. For example, AI-based systems can be trained to recognize children's unique behavioral patterns using historical data collected from studies, such as those focusing on children's performance on touch screens. These systems rely on techniques such as deep neural networks and random forests to analyze behavioral data and classify users with high accuracy.

Additionally, behavioral biometrics is a highly tamperresistant technology, as it relies on real behavioral characteristics that are difficult to manipulate. Thanks to its ability to operate invisibly and be integrated with digital systems, this technology can be used to provide real-time solutions, such as:

- Automatically personalizing content according to age group,
- Activating parental controls based on immediate recognition of a user as a child, and
- Taking preventative measures, such as disabling access to certain content if a user is identified as a child.

The technical challenges facing the field include the accuracy and effectiveness of the models used to distinguish between different age groups, especially in the presence of variable factors — such as children using devices in unconventional ways, or the impact of training on the use of technology. However, the continuous development of machine learning algorithms and big data analysis contributes to reducing these challenges.

Current research primarily focuses on distinguishing between children and adults, which aligns closely with the goals of this study. This targeted approach supports the development of practical, reliable systems that enhance child protection on digital platforms. Consequently, behavioral biometrics offers a specialized, robust, and privacy-conscious tool to safeguard children in the evolving digital landscape, providing sustainable solutions that are resistant to manipulation while ensuring a safe and age-appropriate user experience.

The technical challenges facing the field include the accuracy and effectiveness of models used to differentiate these age groups, especially considering variability in device usage behaviors among children. However, ongoing advancements in machine learning and data analytics are steadily addressing these obstacles, making behavioral biometrics an increasingly viable solution for real-world applications.

2.1 Related Work

Numerous studies have explored the feasibility of using behavioral biometrics to differentiate between children and adults in digital environments, offering promising alternatives to traditional age verification methods. Cheng et al. [3] introduced the iCare system, which employs swipe gestures to classify users by age group. Their method achieved an approximate accuracy of 98.3%, particularly when analyzing multiple consecutive gestures. Similarly, Wani et al. [4] addressed child safety by proposing a biometric model based on social behavior features, reporting an impressive 99.88% accuracy using the PAN 2012 dataset.

Neal and Woodard [5] investigated soft biometric characteristics and behavioral differences in device usage, demonstrating that children's interaction styles significantly differ from those of adults. Extending this perspective, Syed et al. [6] examined environmental factors—such as posture and device size—that impact the reliability of touch gesturebased authentication, and released a new dataset to improve future evaluations.

To expand the scope of behavioral biometrics beyond basic gesture metrics, Abuhamad et al. [7] conducted a broad survey of sensor-based techniques for continuous mobile authentication. They highlighted how features like acceleration and gyroscope data can further enhance age classification systems. Cascone et al. [8] demonstrated that touch keystroke dynamics—such as hold time and inter-key delay—can be leveraged for demographic classification tasks, with potential for real-time implementation.

Emerging trends also emphasize intelligent authentication frameworks that integrate behavioral signals with machine learning. Bansal and Ouda [9] analyzed the potential of reinforcement learning and behavioral biometrics in continuous authentication settings. Their findings suggest that adaptive models improve resilience to behavioral variability. Complementarily, Stylios et al. [10] identified key factors influencing the adoption of behavioral biometrics, such as user trust and perceived security.

Additionally, Finnegan et al. [11] focused on objective measurement of children's mobile device usage through embedded sensors like accelerometers and gyroscopes. Their work demonstrated how motion sensor data combined with machine learning models (Random Forest, k-Nearest Neighbors) can enhance child identification accuracy by capturing device orientation and movement patterns. This approach complements touchscreen biometrics by broadening sensor modalities and improving classification robustness.

Together, these studies illustrate the promise and complexity of behavioral biometrics for child identification and user classification. They underscore the importance of ethical considerations, privacy preservation, and the integration of diverse sensor data to develop robust, scalable, and userfriendly solutions for online child protection and demographic inference.

3. Methodology

To build a reliable and privacy-conscious model for age group classification, the methodology involved designing a gesturebased data collection tool, extracting diverse behavioral features, and applying robust machine learning techniques to distinguish between children and adults based on touchscreen interactions.

3.1 Proposed Methodology

A structured methodology was followed involving several sequential stages to ensure accurate data collection and analysis aligned with the research objectives. First, a customized interactive game was developed to encourage participants to perform diverse touch gestures including tapping, dragging, swiping, and grabbing. The game comprises multiple tasks designed to elicit varied gesture types, capturing comprehensive interaction data.

Participants from various age groups, including children and adults, were recruited to ensure a diverse and representative sample. Informed consent was obtained from all participants, with additional parental consent for minors.

Collected data were analyzed using machine learning techniques, specifically Convolutional Neural Networks (CNN) and Bagging ensemble methods. Key behavioral features such as total touch count, touch pressure, touch frequency, swipe speed, time intervals between touches, distance between touches, and swipe angle were extracted and utilized to build a robust classification model. Figure 1 illustrates the overall structure of the proposed methodology.

3.2 Game design and data collection

Data was collected through a custom interactive game designed to elicit a variety of touch gestures by connecting shapes to their corresponding shadows, naturally triggering taps, swipes, and holds.

The dataset includes the following features:

- Exam Time
- Angle of Drag
- Touch Pressure
- Touch Count
- Touch Frequency
- Time Between Touches
- Distance Between Touches

The output label corresponds to the age category (child = 0, adult = 1). Numeric data were rounded to three decimal places for noise reduction and consistency.

Figure 2 shows the processed data collected from participants.

Figure 1. Structure of the Proposed Methodology

Age	Game Time	Angel of drag	Touch pressure	Touch count	Touch frequency	Swipe speed	Time between touches	Distance between touches

Figure 2. Processed Data Collected from Participants

3.3 Participants Recruitment
Two hundred participants aged 2 to 67 years were recruited from family, friends, and public venues. The sample consisted of 98 children (under 18) and 102 adults (18 or older), providing a balanced dataset to improve model generalizability.

3.4 Gameplay mechanics
Participants were instructed to complete tasks involving a minimum of 16 touch interactions to ensure sufficient data collection within a fixed gameplay duration.

3.5 Gestures metrics
The following metrics were extracted to capture behavioral differences between adults and children:
- Touch Count: Total number of touch events during gameplay, reflecting engagement [12].
- Touch Pressure: Intensity of touch based on gesture speed [13].
- Touch Frequency: Average touches per unit time.
- Swipe Speed: Velocity of swipe gestures [13].
- Time Between Touches: Interval between consecutive touch events [14].
- Distance Between Touches: Physical distance between sequential touches [2].
- Angle of Drag: Directional angle of drag gestures [15].

3.5 Data analysis using machine learning
Data preprocessing included cleaning, normalization, and outlier removal. Two primary algorithms—1D Convolutional Neural Networks (CNN) and Bagging ensembles—were applied to classify users based on touch interaction data.

1) Convolutional Neural Networks (CNN)

CNNs efficiently extract complex patterns from spatial and sequential data. The 1D-CNN model architecture used here is tailored for time-series touch data [16].

2) Bagging Algorithm

Bagging reduces overfitting and improves model stability by aggregating multiple weak learners trained on bootstrap samples, typically decision trees [17].

3.4 Justification for algorithm selection

CNN was chosen for its automatic feature extraction from spatiotemporal data, suitable for subtle touch patterns. Bagging was selected for its ensemble strength to reduce variance and improve robustness given behavioral variability. Preliminary tests confirmed their superior accuracy over traditional classifiers.

4. results and evaluation

The results of the study are presented along with a systematic evaluation of the proposed approach. The objective is to demonstrate the effectiveness of the developed system in capturing user interaction behaviors and to assess the performance of the applied machine learning models. The evaluation begins with a description of the experimental setup, followed by an analysis of the collected data, and concludes with a comparison of model performance across multiple metrics.

4.1 Experimental setup

A field experiment was conducted using a custom interactive game installed on smart devices such as smartphones and tablets. Participants naturally performed various touch gestures including tapping, swiping, scrolling, and dragging. Data-t-on timing, speed, pressure, and gesture direction were automatically recorded without interference to ensure genuine behavior.

Ethical considerations were strict followed with parental consent for minors. The study employé multiple models (CNN and Bagging) to compare effectiveness

4.2 Dataset Description

Participants from diverse age groups were recruited Voluntari and given devices with the pré-installed game. The gameplay involved simple tasks that requière Natural touch gestures. Data was capture invisibly during the session, including pressure, location, timing, and gesture angles.

Data files were antonymie to protêt privacy. The study included 200 participants (98 children under 18, and 102 adults 18 and older). Eich session lastex 5 to 10 minutes to balance data riches and participant confort.

The dataset consisted of détaille behavioral features:

- Number of touches per session • Touch pressure
- Gesture velocity (swipe speed)
- Touch frequency
- Distance between touches
- Time between consecutive touches
- Swipe angle

This Rich feature set ensable capturing nuance differences in user interaction across age groups.

4.3 Model Implementation

Several preprocessing and modeling techniques were employed, including:

- SMOTE (Synthetic Minority Over-sampling Technique) to balance class distribution by creating synthetic minority class samples.
- SMOTETomek, which combines SMOTE with Tomek

Links to refine class boundaries by removing ambiguous points.

- RobustScaler for scaling features robustly against outliers.
- Convolutional Neural Network (CNN) designed for extracting spatial patterns from sequential data.
- Dropout and Early Stopping to reduce overfitting and optimize training.

Models were implemented using Python libraries such as TensorFlow and Scikit-learn.

4.4 Evaluation Metrics

To evaluate classification performance comprehensively, we used:

- Confusion Matrix
- ROC Curve
- AUC (Area Under the Curve)
- Accuracy, Precision, Recall, and F1-score.

4.5 Results and Analysis

Performance metrics included Accuracy, Precision, Recall, and F1-score. Two models were trained and evaluated:

• 1D Convolutional Neural Network (CNN): Utilizing layers such as GlobalAveragePooling1D, Dropout, and Dense for robust feature extraction and classification.

• Bagging Classifier: An ensemble of 50 decision trees combined via majority voting to reduce variance and improve accuracy.

1) CNN Results

Figure 3 illustrates the confusion matrix for the CNN model. The model achieved a high level of classification accuracy, correctly identifying 1,988 children and 1,984 adults. However, it misclassified 11 children as adults and 15 adults as children. This low misclassification rate demonstrates the model's strong generalization capability, even when dealing with real-world behavioral variance.

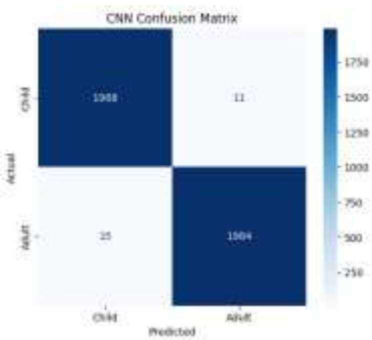

Figure 3. Confusion Matrix of CNN Model

To further assess the model's discriminatory power, Figure 4 presents the ROC curve. The curve is tightly clustered near the top-left corner, indicating near-perfect classification performance. The corresponding AUC value is close to 1.00, confirming that the CNN model performs excellently across different classification thresholds.

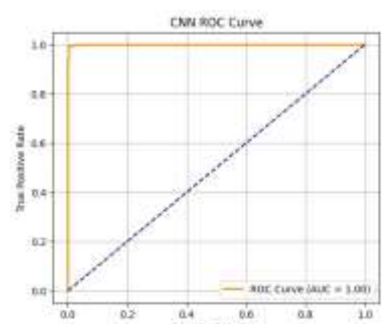

Figure 4. ROC Curve of CNN Model

Quantitatively, Table 1 summarizes the performance metrics for the CNN model. With an accuracy of 98.82% and an F1-score of 0.9882, the model maintains a balanced trade-off between precision and recall, making it suitable for real-time user age classification without requiring additional sensors or identifiers.

Table I. CNN Result

Metric	Value
Accuracy	0.9882
Precision	0.9939
Recall	0.9825
F1-score	0.9882

This result confirms that the CNN model achieves a balanced trade-off between false positives and false negatives, making it effective for real-time classification in practical settings without requiring additional hardware or sensitive inputs.

2) Bagging Results

Figure 5 displays the confusion matrix for the Bagging model. It correctly classified 1,996 children and 1,974 adults. Only 3 children and 25 adults were misclassified. Although the number of adult misclassifications is slightly higher than in CNN, the model overall exhibits stronger accuracy, making it robust for deployment in platforms where false negatives (i.e., undetected children) must be minimized.

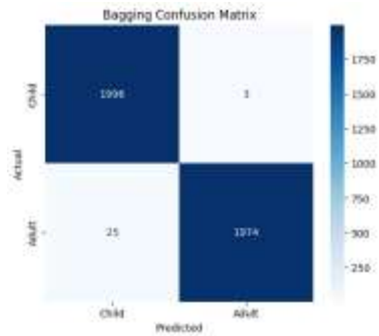

Figure 5. Confusion Matrix of Bagging Model

As shown in Figure 6, the Bagging model's ROC curve also approaches the ideal point of (0,1), reflecting excellent predictive capacity. The nearly perfect AUC confirms the model's strong ability to distinguish between the two user groups.

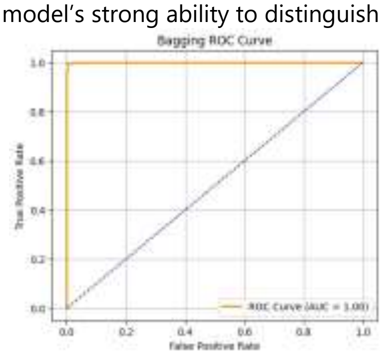

Figure 6. ROC Curve of Bagging Model

Table 2 presents the detailed results of the Bagging model. With a precision of 99.85% and F1-score of 0.993, it surpasses CNN in all metrics, making it the best candidate for age-group detection based solely on behavioral features.

Table II. Bagging Result

Metric	Value
Accuracy	0.993
Precision	0.9985
Recall	0.9875
F1-score	0.993

These values indicate that the Bagging model not only matches but also surpasses CNN in all evaluated metrics, suggesting it as a highly reliable and scalable approach for child detection through behavioral biometrics.

3) Model Comparison

Figure 7 offers a direct visual comparison of the two models across all evaluation metrics. It is evident that the Bagging model consistently outperforms CNN, particularly in precision, which is critical in minimizing false positives in child protection contexts. Overall, both models achieved outstanding results, confirming the viability of using behavioral biometrics for nonintrusive and privacy-preserving user classification. The Bagging model, however, demonstrated a slight performance edge and could be more suitable for real-time deployment in digital safety systems.

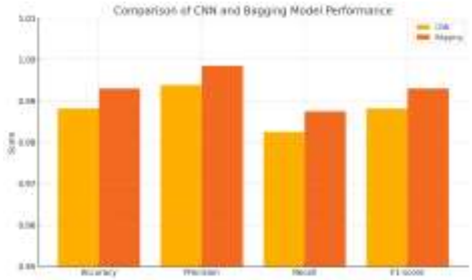

Figure 7. Performance Comparison Between CNN and Bagging Models

5. Discussion

In interpreting the results, it is important to move beyond reporting accuracy values and examine the underlying factors that contributed to the models' effectiveness. Such analysis provides insights into their strengths, potential limitations, and suitability for real-world deployment.

5.1 Model Performance

Our developed models, namely the Convolutional Neural Network (CNN) and the Bagging ensemble classifier, demonstrated remarkable performance in classifying users into children and adults based on their touchscreen behavioral biometrics. The CNN model achieved an accuracy of 98.82%, reflecting its strong capability to automatically extract and learn relevant features from the sequential touch interaction data. Meanwhile, the Bagging model slightly outperformed the CNN with an accuracy of 99.30%, showcasing the robustness gained through aggregating multiple decision trees to reduce variance and overfitting.

In addition to high accuracy, the Bagging model also exhibited superior precision and stability, which are critical metrics for minimizing false positives in real-world child protection applications. This slight performance advantage suggests that ensemble methods can better handle the natural variability and noise inherent in behavioral biometric data. Overall, these results confirm that behavioral biometrics, combined with advanced machine learning algorithms, provide a viable, non-intrusive, and privacy-preserving solution for reliable age group classification on touchscreen devices.

5.1 Comparison With Related Studies

Table 3 provides a concise overview of key studies related to age group classification and child identification using behavioral biometrics. It highlights the focus of each study and the distinct advantages of our approach.

Table III. Summary of Key Related Studies

Study	Focus	Main Strengths of this Approach
Cheng et al. [3]	Child detection via touch gestures using classical ML, 98.3% accuracy	Deeper behavioral features, CNN+Bagging, higher accuracy
Liang et al. [18]	Behavioral biometrics for IoT continuous authentication, no experimental results	Real system, 99% accuracy, interactive game data
Guimarães et al. [19]	Age classification via social media text, 95% accuracy	Non-intrusive touch data, better privacy, higher accuracy
Zaccagnino et al. [20]	Gesture-based child safety tech, 88% accuracy	More diverse dataset, interactive tasks, 99.3% accuracy
Neal & Woodard [5]	Soft biometrics from 5]app usage with variable accuracy	Focused task, higher accuracy, better privacy
Finnegan et al. [11]	Objective mobile use metrics with sensors	Innovative metrics, empirical evidence, improved understanding

Although the table summarizes the key points briefly, several important aspects from these studies merit further discussion:

- Cheng et al. [3] employed classical machine learning algorithms like kNN and SVM on limited gesture features such as hand geometry and finger dexterity. In contrast, our model utilizes deeper behavioral features including swipe angle, speed, and pressure, combined with powerful CNN and Bagging methods, resulting in significantly improved accuracy.
- Liang et al. [18] provided a comprehensive review on IoT continuous authentication but lacked experimental validation. We complement this by implementing a working system that collects real-world behavioral data through an interactive game, achieving over 99% accuracy.
- Guimarães et al. [19] focused on age classification using textual data from social media posts, which raises privacy concerns. Our approach relies solely on non-intrusive touch gestures, enhancing privacy and enabling easier deployment in child-safe applications, while improving accuracy beyond 99%.
- Zaccagnino et al. [20] presented techno-regulation through gesture analysis on a relatively small and less diverse dataset. Our study addresses this gap by using a more varied dataset from 200 participants engaging in interactive tasks, achieving superior accuracy and AUC scores.
- Neal and Woodard [5] explored soft biometrics such as app usage and calls, facing accuracy fluctuations and privacy issues. Our method narrows the focus to child vs. adult classification with more stable and higher accuracy, while respecting privacy by excluding sensitive data like calls or messages.
- Finnegan et al. [11] introduced novel behavioral metrics using embedded sensors like accelerometers and gyroscopes to objectively measure children's device usage. This complements touchscreen biometrics by broadening sensor modalities and supporting improved child identification robustness.

Collectively, these studies demonstrate the evolving landscape of behavioral biometrics for child identification. Our approach advances this field by combining interactive data collection, sophisticated modeling, robust preprocessing, and privacy preservation, culminating in a scalable solution ready for real-world application.

5. Conclusion and Future Work

This study proposed a novel, privacy-preserving framework for distinguishing children from adults based on touchscreen behavioral biometrics. By collecting diverse gesture data through an interactive game and extracting a rich set of features—such as pressure, speed, angle, and timing—we trained two machine learning models, CNN and Bagging, which achieved high accuracies of 98.82% and 99.30%, respectively. The combination of diverse behavioral features, effective preprocessing, and robust modeling contributed to the system's superior performance and demonstrated the feasibility of using touch-based interactions for real-time age group classification.

Future work may involve expanding the participant pool across more diverse demographics and device types to enhance model generalizability. Additional gesture types, such as multi-touch and rotational inputs, could further improve feature richness. Investigating temporal models (e.g., LSTM), integrating the system as à background service for continuous classification, and analyzing behavioral changes over time—particularly in children—will strengthen the system's adaptability and support broader applications in digital child safety.

Acknowledgment: This research is funded by the Deanship of Graduate Studies and Scientific Research 934 at Qassim University (QU-APC-2025)".

Conflicts of Interest: "The authors declare no conflict of interest."

Sulaiman Al Amro – [ORCID iD: 0000-0002-5027-6967]

References

[1] IEEE Standards Association, "Ieee sa works toward safer, ageappropriate internet for kids," https://standards.ieee.org/beyond-standards/online-age-verification-program/, 2025, accessed: 2025-05-30.

[2] R.-D. Vatavu, G. Cramariuc, and O.-A. Schipor, "Touch interaction for children aged 3 to 6 years: Experimental findings and relationship to motor skills," International Journal of Human-Computer Studies, vol. 74, pp. 54– 76, 2015.

[3] Y. Cheng, X. Ji, X. Li, T. Zhang, S. Malebary, X. Qu, and W. Xu, "Identifying child users via touchscreen interactions," ACM Transactions on Sensor Networks (TOSN), vol. 16, no. 4, pp. 1–25, 2020.

[4] M. A. Wani, N. Agarwal, and P. Bours, "Sexual-predator detection system based on social behavior biometric (ssb) features," Procedia Computer Science, vol. 189, pp. 116–127, 2021.

[5] T. J. Neal and D. L. Woodard, "You are not acting like yourself: A study on soft biometric classification, person identification, and mobile device use," IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 1, no. 2, pp. 109–122, 2019.

[6] Z. Syed, J. Helmick, S. Banerjee, and B. Cukic, "Touch gesture-based authentication on mobile devices: The effects of user posture, device size, configuration, and inter-session variability," Journal of Systems and Software, vol. 149, pp. 158–173, 2019.

[7] M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, "Sensorbased continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey," IEEE Internet of Things Journal, vol. 8, no. 1, pp. 65–84, 2020.

[8] L. Cascone, M. Nappi, F. Narducci, and C. Pero, “Touch keystroke dynamics for demographic classification,” Pattern Recognition Letters, vol. 158, pp. 63–70, 2022.
[9] P. Bansal and A. Ouda, “Continuous authentication in the digital age: An analysis of reinforcement learning and behavioral biometrics,” Computers, vol. 13, no. 4, p. 103, 2024.
[10] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, “Key factors driving the adoption of behavioral biometrics and continuous authentication technology: an empirical research,” Information & Computer Security, vol. 30, no. 4, pp. 562–582, 2022.
[11] O. L. Finnegan, R. G. Weaver, H. Yang, J. W. White, S. Nelakuditi, Z. Zhong, R. Ghosal, Y. Tong, A. B. Cepni, E. L. Adams et al., “Advancing objective mobile device use measurement in children ages 6–11 through built-in device sensors: A proof-of-concept study,” Human Behavior and Emerging Technologies, vol. 2024, no. 1, p. 5860114, 2024.
[12] M. B. Cano, P. Perry, R. Ashman, and K. Waite, “The influence of image interactivity upon user engagement when using mobile touch screens,” Computers in Human Behavior, vol. 77, pp. 406–412, 2017.
[13] S.-C. Lu, P. Rowe, C. Tachtatzis, I. Andonovic, A. Anzulewicz, K. Sobota, and J. Delafield-Butt, “Swipe kinematic differences in young children with autism spectrum disorders are task-and age-dependent: A smart tablet game approach,” Brain Disorders, vol. 5, p. 100032, 2022.
[14] J. Kong, M. Zhong, J. Fogarty, and J. O. Wobbrock, “New metrics for understanding touch by people with and without limited fine motor function,” in Proceedings of the 23rd International ACM SIGACCESS Conference on Computers and Accessibility. ACM, 2021, pp. 1–4.
[15] S. A. Mascaro and H. H. Asada, “Measurement of finger posture and threeaxis fingertip touch force using fingernail sensors,” IEEE Transactions on Robotics and Automation, vol. 20, no. 1, pp. 26–35, 2004.
[16] Z. Li, F. Liu, W. Yang, S. Peng, and J. Zhou, “A survey of convolutional neural networks: analysis, applications, and prospects,” IEEE transactions on neural networks and learning systems, vol. 33, no. 12, pp. 6999–7019, 2021.
[17] J. Awujoola Olalekan, F. Ogwueleka, and P. Odion, “Effective and accurate bootstrap aggregating (bagging) ensemble algorithm model for prediction and classification of hypothyroid disease,” International Journal of Computer Applications, vol. 975, p. 8887, 2020.
[18] Y. Liang, S. Samtani, B. Guo, and Z. Yu, “Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective,” IEEE Internet of Things Journal, vol. 7, no. 9, pp. 9128–9143, 2020.
[19] R. G. Guimaraes, R. L. Rosa, D. De Gaetano, D. Z. Rodriguez, and G. Bressan, “Age groups classification in social network using deep learning,” IEEE Access, vol. 5, pp. 10805–10816, 2017.
[20] R. Zaccagnino, C. Capo, A. Guarino, N. Lettieri, and D. Malandrino, “Techno-regulation and intelligent safeguards: Analysis of touch gestures for online child protection,” Multimedia tools and applications, vol. 80, pp.15803–15824, 2021.