IRSTI 28.23.19 **https://doi.org/10.58805/kazutb.v.4.29-1231**

USER AUTHENTICATION IN MOBILE LEARNING: BEHAVIORAL ANALYSIS WITH GYROSCOPE AND ACCELEROMETER DATA

B.B. Serbin, A.M. Kassenkhan, R.K. Uskenbayeva, Zh.B. Kalpeyeva
Satbayev university, Almaty, Kazakhstan
Corresponding author: a.kassenkhan@satbayev.university

With rising popularity of mobile devices and increasingly voluminous learning data, securing individual information has become a matter of urgency. This work proposes a behavioral authentication model that reinforces access security on smart learning platforms through learning user behavior from accelerometer and gyroscope data. Designed to suit mobile learning environments where voluminous user interaction with interactive content necessitates trustworthy authentication processes, this model reinforces access security on smart learning platforms through learning user behavior from accelerometer and gyroscope data. Beyond taking into consideration accessible authentication processes, this paper further presents an innovative solution designed to suit mobile environments. Experiment results prove the model to be viable in upkeeping data integrity as well as securing user access to school systems.

Keywords: smartphone, mobile application, behavioral model, authentication, gyroscope, accelerometer, security, education.

МОБИЛЬДІ ОҚЫТУДАҒЫ ПАЙДАЛАНУШЫЛАРДЫ АУТЕНТИФИКАЦИЯЛАУ: ГИРОСКОП ПЕН АКСЕЛЕРОМЕТР ДЕРЕКТЕРІН ПАЙДАЛАНА ОТЫРЫП, МІНЕЗ-ҚҰЛЫҚТЫ ТАЛДАУ

В.В. Сербин, А.М. Қасенхан, Ж.Б. Кальпеева, Р.К. Ускенбаева
Satbayev University, Алматы, Қазақстан,
e-mail: a.kassenkhan@satbayev.university

Мобильді құрылғыларды кеңінен қолдану және білім беру деректерінің көлемінің артуына байланысты жеке ақпаратты қорғауды өзекті мәселеге айналды. Бұл зерттеуде пайдаланушылардың мінез-құлық үлгілерін гироскоп пен акселерометр деректері арқылы талдау негізінде интеллектуалды білім беру платформаларына қол жеткізудің қауіпсіздігін арттыратын мінез-құлыққа негізделген аутентификация үлгісі ұсынылады. Модель мобильді оқыту ортасына арнайы бейімделген, мұнда пайдаланушының динамикалық мазмұнмен жиі өзара әрекеттесуі сенімді аутентификация механизмдерін талап етеді. Қолданыстағы аутентификация әдістеріне шолу жасаумен қатар, зерттеу мобильді қолдануға арналған жаңа тәсілді ұсынады. Алынған нәтижелер бұл үлгінің деректердің тұтастығын қамтамасыз ету және білім беру жүйелерінде пайдаланушылардың қолжетімділігін қорғау тиімділігін көрсетеді.

Түйін сөздер: смартфон, мобильді қосымша, мінез-құлық моделі, аутентификация, гироскоп, акселерометр, қауіпсіздік, білім.

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ В МОБИЛЬНОМ ОБУЧЕНИИ: ПОВЕДЕНЧЕСКИЙ АНАЛИЗ С ИСПОЛЬЗОВАНИЕМ ДАННЫХ ГИРОСКОПА И АКСЕЛЕРОМЕТРА

В.В. Сербин, А.М. Қасенхан, Ж.Б. Кальпеева, Р.К. Ускенбаева
Satbayev University, Алматы, Казахстан
e-mail: a.kassenkhan@satbayev.university

Популярность мобильных устройств и растущий объём учебных данных превратили защиту персональных данных в актуальную проблему. В данном исследовании представлена поведенческая модель аутентификации, повышающая безопасность доступа на интеллектуальных обучающих платформах путём анализа поведения пользователей на основе данных гироскопа и акселерометра. Модель адаптирована к условиям мобильного обучения, где интенсивное взаимодействие

пользователя с интерактивным контентом требует надёжных механизмов аутентификации. Помимо рассмотрения существующих методов аутентификации, в данной статье также представлено новое решение, адаптированное для мобильных сред. Результаты демонстрируют эффективность модели в сохранении целостности данных и обеспечении безопасности доступа пользователей в школьных системах.

Ключевые слова: смартфон, мобильное приложение, поведенческая модель, аутентификация, гироскоп, акселерометр, безопасность, образование.

Introduction. This widespread adoption of smartphones and mobile technologies has been no less influential in contemporary teaching and learning, changing how students learn, interact, and interact with learning content. m-learning platforms like Moodle, Coursera, and Edmodo provide flexible access to personalized learning content to students, facilitate real-time collaboration, and allow constant monitoring of progress-frequently without regard to time or place.

Nevertheless, this growing use of mobile instruments comes along with new and multifaceted security issues. Among those are issues of how to protect user information, authenticate identity, as well as provide limited access to learning platforms. It becomes essential to ensure that only authenticated users are capable of accessing and interacting within online learning environments as much as privacy, customization, and learning integrity are all on the line.

Conventional authentication methods-such as passwords, PINs, or even biometric identifiers-usually fail in mobile learning environments. Passwords are subject to weakness, reusing of passwords, and being broken, and biometric devices such as face or finger recognition might encounter technological constraints or user Wariness about privacy. Additionally, all of these systems only authenticate humans once upon login, providing no protection if access is gained illicitly during session.

While privacy is broadly thought to be a requirement in mobile app development, as yet most users would rather have convenience. For instance, a cross-country survey conducted by Schewina et al. (2024) indicated that data-gathering apps were routinely differently favourably ranked even when privacy risk was recognised. This reflects a requirement for authentication mechanisms that are as much a pleasure to use as they are secure-particularly in online learning environments where users transact regularly and interactively [1].

One of such promising remedies is behavioral authentication (BA) that is based on monitoring how an individual interacts with his device. Such behaviors as touch gestures, tilting of a device, swiping, and motion patterns are distinctive to users and hard to counterfeit. Integrated phone sensors in a smartphone (gyroscopes and accelerometers) allow for capturing such subtle behaviors in real time, providing unobtrusive and context-aware identity verification. Such a method can be an effective complement to regular login processes.

Cybersecurity of online learning is further informed by user awareness and practice. According to a study conducted by Kocsis et al. (2025), students trained in digital hygiene significantly better identified and evaded online incidents such as phishing or abuse of authentication tools. This suggests that good technical systems should be reinforced by user training [2].

Even as biometric instruments have been increasingly employed in areas of communications as diverse as cell phone payments, apprehension regarding user trust and usability of systems persists. A scaled-up study by Liébana-Cabanillas et al. (2024) spanning more than 2,500 users indicated a number of principal psychological and contextual variables that affect whether users accept biometric verification. Their findings revealed that performance expectations, perceived ease of use, and risk perception significantly impact user choice. These findings further drive home a point that is especially true in learning environments where manned user activity is recurrent and sensitive [3].

During the last two decades, behavioral

authentication has attracted significant attention in academia as well as in industry. A keyword search of “behavioral authentication” and “mobile learning” on ScienceDirect illustrates this trend: publications of this type have leapt from 25 in 2002 to 1,484 in 2024. By mid-2025, only 1,351 articles had been indexed but this number may reach 2,700 or higher by year-end. This exponential growth betrays growing interest in security systems driven by behavior as technological potential and confidentiality requirements expand.

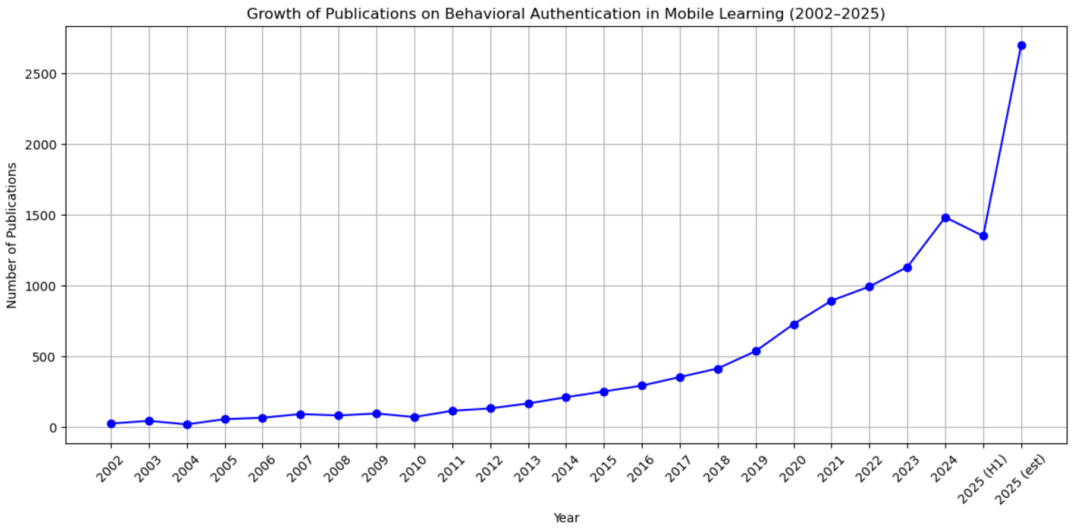


Fig 1 - Annual number of publications on ”behavioral authentication” and ”mobile learning” (2002–2025)

Increased interest in behavioral authentication is being spurred on by a number of converging trends. These range from an accelerating adoption of sensor-enabled mobile devices to a worldwide online-education binge set off by the COVID-19 virus to growing cybersecurity and data-protection priorities in online learning environments. Taken as a whole, these trends create a strong requirement for flexible yet trustworthy authentication systems that protect user identity without a loss of usability.

To promote efficient resolution of these challenges, this current work proposes a behavioral authentication framework that incorporates motion sensor information from smartphones-namely, output from accelerometers and gyroscopes. With mobile learning environments as its context of reference, the system aims to promote a reinforcement of security as well as usability through an examination of users’ distinctive motion patterns. With behavioral profiling and machine learning processes as its integrating principles, this suggested solution provides ongoing, context-aware, and transparent authentication that is in conformity with today’ s changing learning platforms’ needs.

Literature Review.

1. Input-Based Behavioral Features

Behavioral authentication (BA) techniques that employ input-based attributes-such as touch interactions and typing behavior-have proven significant promise for real-time user identification on mobile devices. Characteristics such as touchscreen gestures and keystroke dynamics capture unique and frequently difficult-to-imagine user interaction patterns.

Sejjari et al. (2024) recently assessed employing swiping motions to authenticate users persistently on smartphones. Their deep learning system demonstrated an exceedingly low Equal Error Rate (EER) of 0.20%, as it is possible to visualize gesture-based biometry as a potential method of persistent identity authentication [4]. In a similar vein, Lim et al. (2024) explored touchstroke kinetics by considering variables like swipe velocity, pressure, and duration. Employing interpretable

machine learning frameworks-such as decision trees and random forests—their interpretable machine learning models realized EERs ranging from 0.02% to 0.07%. Explaining their AI system as explainable provides a good compromise between achieving high performance as well as having interpretable models [5].

Typing patterns on soft keyboards have also been promising behavioral user profiling. Sağbaş and Ballalı (2024) integrated keystroke dynamics into motion sensor data to capture tiny shifts in grip as well as device micro-movements. Their feature-rotation of correlation-based feature selection as well as logistic regression-based hybrid solution offered 93% classification accuracy along with sub-millisecond time to process, indicating good potential for real-time mobile application [6].

2. Motion-Based Behavioral Features.

Behavior-based motion features-gathered through accelerometers, gyroscopes, and magnetometers-have been a prominent area of focus within continuous authentication. This is mainly because motion sensors have increasingly been a part of smartphones and wearable technology, enabling it to be possible to stealthily capture user behavior in real time.

In a typical example, Mekruksavanich and Jitpattanakul (2024) offered SE-DeepConvNet, a convolution network enriched with squeeze-and-excitation modules. Tested on gait activities from the USC-HAD dataset, the model scored a perfect classification score of giving 100% accuracy and a 0% Equal Error Rate (EER) [7]. In yet another work, Alawami et al. (2024) provided MotionID-a motion-authentication system designed to operate under real operational conditions, considering sensor noise as well as sampling variations. Their system scored an F1-value of as much as 98.5% under controlled environments and about 90% in more varied real-world environments [8].

Gait-anchored identification methods have come under consideration as well. Kokal et al. (2024) employed ensemble classifiers such as Random Forest and XGBoost to discern users from their gait patterns. Their results indicated strong classification accuracy, even if the authors did promote further testing under wider real-world situations [9]. To supplement this, Cariello et al. (2024) set out SMARTCOPE-a context-aware system that automatically detects when a device is being passed from user to user. The system significantly decreased the EER from 7.8% to 4.6% while compressed its intrusion into the user experience to a minimum [10].

Later, transformer-based frameworks have been used in motion-based authentication. Li et al. (2024) proposed FuMeAuth that fused accelerometer, gyroscope, and magnetometer signals by memory-augmented Transformer networks. Their network stated 99.84% accuracy and a 0.14% EER on large-scale datasets [11]. Along a similar line, Delgado-Santos et al. (2023) proved that CNN and RNN-based methods were outclassed by gait biometric tasks by employing whuGAIT and OU-ISIR datasets [12]. Continuing their work further, the authors in a subsequent work put forward M-GaitFormer as a model that only used accelerometer and gyroscope signals. This system provided better performance compared to traditional methods as it reached an EER of 3.42% and 2.90% on benchmark datasets [13].

3.Machine Learning Architectures for Behavioral Authentication.

Deep learning and machine learning methods of an advanced order are increasingly being used to extract and represent behavioral patterns to be used as authenticators. Vision Transformer (ViT)-motivated architecture methods and hybrid learning models are increasingly picking up steam because of their multimodal and sequential sensor data tackling abilities.

Alotaibi and Alotaibi (2025) proposed a hybrid architecture that converts motion sensor inputs into patch-like patches to be processed through a multi-head attention mechanism and BiLSTM network combination. Their architecture realized classification accuracy of 97.51% on MotionSense and 89.37% on UCI HAR data with good generalizability across a variety of activity realms [14].

Following further development on generative methods, Li et al. (2024) suggested MAuGANs as a new hybrid system that integrates memory-augmented autoencoders along with generative adversarial networks that employ Transformers. Generating Synthetic Impostor Samples (SIPS) this model reached a 99.65% accuracy and 0.33% EER when validating on unseen users beforehand [15]. Likewise, Delgado-Santos et al. (2024) indicated SwipeFormer as a Transformer-based Swipe Gesture Analysis Model that surpassed traditional baselines on benchmark and realistic datasets alike [16].

To tackle the challenge of behavioral drift as time progresses, Shen et al. (2024) proposed IncreAuth as an incremental learning system that combined gradient-boosted decision trees and deep neural networks. This model remained stably authenticatable on unconstrained datasets, wherein user behavior could change drastically [17].

Yang et al. (2024) made a suggestion of CALL, an unsupervised authentication system that utilizes low-rank Transformers and spatial ranking techniques. The system realized Equal Error Rates of 3.86%, without labeled training data [18]. To effectively tackle the trivial problem of a scarcity of impostor data, Li et al. (2024) suggested AEGANAuth having a CVAE-GAN architecture and error measures of reconstruction, to realize a classification accuracy of 97.85% [19].

Nguyen et al. (2024) provided BehaveFormer, a dual-attention Transformer network tailored for multichannel time-series sensor data. They generated systems that resulted in less than 3% EER for keystroke- and swipe-based authentication tasks [20]. Meanwhile, Kumari et al. (2023) made use of conventional ensemble classifiers-old girl(Random Forest and LightGBM-to sensor data gathered from a number of body positions. Their system reached a maximum of 98.8% accuracy as it optimized performance by employing Recursive Feature Elimination (RFE) [21].

4. Applications in Education and Emerging Modalities.

Behavioral authentication methods have been further attempted in teaching and cognitive monitoring situations. For example, Gunawardena et al. (2023) made a survey of portable eye-tracking systems with a view to their application in teaching situations while meanwhile pointing out drawbacks concerned with complexity of calibration and sensibleness of hardware [22].

In another context, Nosrati et al. (2024) proposed a voice-based bank-based authentication system that proved highly robust against background noise as well as speaker orientation variations. Mel-frequency cepstral coefficients (MFCCs) along with fuzzy support vector machines (SVMs) optimized by metaheuristic algorithms were employed in this system to yield an accuracy of 98.29% [23].

Cao et al. (2024) proposed HandKey, a new keyless entry system from distinctive vibration patterns caused by door knock gestures. As a variant, HandPass (Cao et al., 2023) also took advantage of natural hand-device interactions and matching vibration outputs to realize passive user verification. Both techniques demonstrated strong spoof-attack resistance and thus have a promising application in safe access systems [24, 25].

Zhang et al. (2023) put forward a multi-sensor authentication system that combined physiological and behavioral signals. Their system utilized Kalman filtering to improve signals and deployed Siamese neural networks to achieve similarity scoring. It provided a promising blend ofstrength and userfriendliness that proved especially good in situations where signal ruthlessness could be an issue [26].

5. Challenges and Limitations.

Even from significant breakthroughs, behavioral authentication systems have yet to evade a set of technical and practical difficulties. Principal among these are sensor-level noise, behavioral long-term drift, susceptibility to adversarial manipulation, and a lack of available impostor data under field conditions.

To cope with such issues, Chen et al. (2024) put forward SSPRA as an input perturbation resistance system. By embedding dual fusion mechanisms and Markov modeling, SSPRA proved stronger

resistance to zero-effort intrusions as well as against selective attacks and proved promising in its safer application in changing environments [27].

Beyond authentication itself, trust assessment in mobile environments has increasingly been a subject of investigation. While indirectly concerned with behavioral biometrics, Li and Li' s (2024) framework is pertinent. Their principle-assumptions model of distributed trust control is centered on adaptive reliability and contextual risk assessment-ideas that might guide further work in developing more sophisticated and adaptive behavioral authentication systems [28].

Materials and Methods. This section gives an elaborate explanation of mathematical formulas used in this work besides developing a logical approach to calculating important performance parameters (IPPs). It also presents computational approach as well as decision-making algorithms used in user authentication within the mobile application.

The section comprises systematic analysis of logic behind computation of KPI, detailing stepwise working of information processing flow along with incorporation of algorithm that enables efficient and precise verification of users. By integrating theoretical modeling along with applied algorithmic approach, the section reveals approach adopted in a systematic mode to enhance reliability of mobile authentication system along with its overall performance.

1. Behavioral Data Collection Using Smartphone Sensors.

Smartphone sensors, especially accelerometers and gyroscopes, play a central role in behavioral authentication systems by registered motion and orientation information that indicate person-specific patterns of device usage. The accelerometer is responsible for linear acceleration along three axes of space (X, Y, and Z) so that it is possible to register displacements of the device position and user-elicited movements. These signals are used to deduce how a user usually holds and handles a device when it is put into common use.

Gyroscope, meanwhile, estimates angular velocity to impart refined information about rotational activity of the device. This information is particularly significant to estimate orientation of the screen and spatial orientation. When combined together, accelerometer and gyroscope inputs allow drawing of rich behavioral features upon which authentication model is constructed.

2. Device Parameters and Correlation Coefficients.

Pearson correlation coefficient to estimate linear associations between variables and is core to the decision-making algorithm. There are two forms of sensor input that this model incorporates: gyroscope data and accelerometer data. The aggregate correlation coefficient (labeled k) is an expression of combined sensor effect and is computed through Equation (1):

$$k = \frac{1}{2}(k_g + k_a) \tag{1}$$

k - general correspondence coefficient;

k_g - gyroscope correlation coefficient;

k_a - accelerometer correlation coefficient.

At the initial step, we will find an individual correlation of accessible indicators -accelerometer and gyroscope. As it is equal to three parameters of the gyroscope (X, Y, and Z axes) of the overall gyroscope, its preliminary weight of a correlation will be defined by Equation (2).

$$k_g = \frac{1}{3}(k_x + k_y + k_z) \tag{2}$$

where,

k_x - correlation coefficient of the gyroscope' s X-axis;

k_y - correlation coefficient of the gyroscope' s Y-axis;

k_z - correlation coefficient of the gyroscope' s Z-axis.

Calculated from Equation (3) is the correlation of each parameter:

$$k_x = \frac{x_{avg} * x}{\sigma_{x_2}\sigma_{x_1}} \tag{3}$$

This is an example of a calculation of a correlation of a X-axis as follows:

x_{avg} - the average value of all X-axis readings in a single test;

x - the initial X-axis value during testing;

σx_1 - the standard deviation of the first test value;

σx_2 - the standard deviation of the second test value.

3. Population Standard Deviation.

To determine the overall correlation, we should first work out a standard deviation of each of the parameters that come into question. Standard deviation is a basic statistics measure that expresses a number to measure how much a collection of variants varies from its mean. It indicates how much individual numbers bear from a mean of a distribution.

Mathematically, it is given as the positive square root of the mean of squares of all difference of each number from the mean of a dataset. For example, the mathematical expression of population standard deviation is as follows: in Equation (4) below.

$$\sigma = \frac{\sqrt{\sum_{i-1}^{n} (x_i - x_{avg})^2}}{n-1} \qquad (4)$$

where,

n - number of experimental values;

x_i - experimental value;

$\sum_{i=1}^{n} x_i$ - sum of experimental values.

2. To compute mean deviation of two compared parameters of a given parameter (first and second) from their calculated average, each is subtracted from the mean. Obtained differences thus give an estimate of mean deviation of the first indicator. This is expressed formally in Equation (5) below.

$$x_i - x_{avg} \qquad (5)$$

These steps present the format of procedure to compute the population standard deviation of each parameter:

1. The previously calculated deviation values (as provided in Equation 5) are squared.

2. The squared residuals of all test samples of the parameter are added up.

3. The end result is then divided by how many test samples have been made.

4. The square root of this ratio is then found to give you the standard deviation (don’ t mistake this figure as variance which is its unsquared self).

5. The same procedure is done separately for every parameter – affects Y-axis, Z-axis, as well as accelerometer information.

After having calculated all appropriate parameters’ population standard deviation, we will compute a correlation coefficient to each parameter by Equation (3). We will then do the same calculation to gyroscope axes three by Equation (2). We will then sum up results by Equation (1) to give us the overall correlation measure.

4. Decision making algorithm.

Decision-making algorithm is based on the Pearson correlation coefficient, which is a statistical parameter that measures how strong and in which direction a linear relationship between two variables is. It varies from -1 to +1: a result of +1 denotes a perfect linear positive correspondence, 0 denotes no linear correspondence, and -1 denotes a perfect linear negative correspondence.

For this work, a correlation coefficient near +1 is most desirable because it indicates a strong linear positive relationship between correlated parameters that are being compared. This threshold serves as a basis of user authentication thresholds. Interpretations of Pearson correlation values employed in this system are tabulated in Table 1.

Experimental work

To test the given hypothesis, a number of large experiments have been simulated.100 test users have been divided into five groups of 20 users each.

Since sensor measurements could be subject to variations depending on situations, measurements were made on five controlled situations to determine variations in the X, Y, and Z coordinate positions. These situations are explained as below:

- Phone sitting on a plane: Coordinate values associated will be given in Table 2.

- Phone user in a user-held station: Table 3 presents the data.

- User in a sitting posture: These X, Y, and Z values are tabulated in Table 4.

- User reclining: Table 5 has recorded coordinate data.

- User moving at a speed of 4–5 km/h: The measurements of dynamometer are tabulated in Table 6.

Table 1 - Decision making

Correlation coefficient range	Decision
If (k 0.5)	User identified
If (k 0.5) and (k 0)	User identity is questionable
If (k 0)	User not identified

Table 2 - Condition 1. When the phone is on the surface

Group	X_{avr}	Y_{avr}	Z_{avr}	A_{avr}
1	+0.01	0.00	0.00	0.01
2	0.00	+0.015	0.00	0.00
3	-0.01	0.00	0.00	0.00
4	0.00	0.00	0.01	0.00
5	0.00	-0.01	+0.01	0.00

Table 3 - State 2. When a person holds the phone stationary (0 km/h)

Group	X_{avr}	Y_{avr}	Z_{avr}	A_{avr}
1	+0.03	+0.02	+0.01	1.32
2	-0.5	-0.06	+0.02	2.6
3	-0.04	+0.08	-0.04	1.87
4	+0.06	-0.03	+0.03	2.63
5	+0.09	+0.02	-0.05	1.1

Table 4 - State 3. When a person is sitting

Group	X_{avr}	Y_{avr}	Z_{avr}	A_{avr}
1	+0.01	-0.05	+0.04	0.37
2	+0.03	-0.06	+0.05	0.78
3	+0.02	-0.08	+0.04	0.63
4	-0.01	-0.07	+0.05	1.02
5	+0.02	-0.06	+0.05	0.86

Table 5 - Condition 4. When a person lies

Group	X_{avr}	Y_{avr}	Z_{avr}	A_{avr}
1	+0.01	-0.15	+0.06	1.10
2	-0.08	-0.11	-0.01	1.35
3	-0.07	-0.13	+0.05	1.32
4	-0.10	-0.16	+0.04	1.56
5	-0.11	-0.25	+0.03	1.24

Table 6 - Condition 5. When a person walks at an average speed of 4-5 km/h.

Group	X_{avr}	Y_{avr}	Z_{avr}	A_{avr}
1	-0.16	-0.35	+3.05	2.93
2	+1.23	+2.28	+1.76	3.05
3	+0.18	+1.86	+0.97	2.35
4	-1.36	+2.32	-2.17	2.12
5	+0.29	+0.96	+0.56	1.98

Experimental results revealed that Condition 2—if users keep their phones in their hands—is the most appropriate situation to effectively estimate the correlation coefficient. When this condition is set, behavioral signals are strong and distinctive enough to facilitate safe user identification.

To compare the effectiveness of the authentication approach, correlation coefficients were compared under each experiment condition. Result is divided into two test cases:

Case 1: Same user signs into the system twice.

Case 2: When two different users login to access the system.

Condition 1: Repeated login by the same user

Step 1: Computation of the correlation coefficient of the X-axis from two login attempts of a same user.

Step 2: It is calculated by the formulas below:

1) The mean deviation is: $x_{avg} = -5,264 - 3,44 = 1,06$;

2) Variance $= x_2 = 1.06^2 = 1.13$;

3) Square of the two mean deviations of the test values: $= 1,13 * 1,111069206 = 1,1215880186$.

Calculating the X-axis correlation of the same person.

$$k_x = \frac{x_{avg} * x}{\sigma_{x_2} * \sigma_{x_1}} = 0,757535214$$

Calculating the Y-axis correlation

$$k_y = \frac{y_{avg} * y}{\sigma_{y_2} * \sigma_{y_1}} = 0,7633229$$

Calculation of correlation along the Z axis:

$$k_z = \frac{z_{avg} * z}{\sigma_{z_2} * \sigma_{z_1}} = 0,08977132$$

4) Total correlation coefficient:

$$k_g = \frac{1}{3}\left(k_x + k_y + k_z\right) = \frac{1}{3}(0,757535214 + 0.7633229 + 0.08977132) = 0,806190438$$

Calculation of correlation A:

$$k_a = \left(\frac{A_{avg} * A}{\sigma_{A_2} * \sigma_{A_1}}\right) = 0,524778876$$

General ratio of one person:

$$k = \frac{1}{2}\left(k_g + k_a\right) = \frac{1}{2}(0,806190438 + 0,524778876) = 0,665484657$$

Condition 2. When two different people enter the system.
Calculate X-axis correlation.

$$k_x = \frac{x_{avg} * x}{\sigma_{x_2} * \sigma_{x_1}} = 0,131932012$$

Calculating the Y-axis correlation:

$$k_y = \frac{y_{avg} * y}{\sigma_{y_2} * \sigma_{y_1}} = 0,405104411$$

Calculating the correlation along the Z axis:

$$k_z = \frac{z_{avg} * z}{\sigma_{z_2} * \sigma_{z_1}} = 0,130146264$$

4) Total correlation coefficient:

$$k_g = \frac{1}{3}\left(k_x + k_y + k_z\right) = \frac{1}{3}(-0,131932012 + 0.405104411 + 0.130146264) = 0,403318663$$

Calculation of correlation A:

$$k_a = \left(\frac{A_{avg} * A}{\sigma_{A_2} * \sigma_{A_1}}\right) = 0,497473449$$

General ratio of two people:

$$k = \frac{1}{2}\left(k_g + k_a\right) = \frac{1}{2}\left(0,403318663 + (-0,497473449)\right) = -0,047077393$$

The hypothesis was tested through a series of large-scale experiments involving five groups of 20 participants each. Sensor data were collected under five controlled conditions:

1. when the phone was placed on a flat surface,
2. when held stationary by the user,
3. when the user was seated,
4. when lying down, and
5. while walking at a speed of 4-5 km/h.

Among these situations, highest correlation coefficients were regularly found under Condition 2-the user standing completely still to hold the phone-in signalling it as the most convenient setting to achieve good user authentication.

To compare the system performance, two principal cases have been obtained from dividing test results:

- Case 1: The same individual logged into the system twice.

- Case 2: Two different individuals attempted to log in.

For all of these conditions and test cases, we calculated a set of correlation coefficients along the X, Y, and Z axes as well as accelerometer magnitude (A) axes. Individual measurements from these were subsequently aggregated to compute an overall correlation coefficient so that an all-inclusive behavioral similarity analysis could be conducted across situations.

Results and Discussions. This work explored the possibility of employing motion-based user authentication from smartphone sensor data, namely from gyroscope and accelerometer sensors. Three different user situations: resting, standing, and walking, were chosen as situations to be evaluated. Results proved that phone location is of decisive importance to authenticate device accuracy. Of all evaluated cases, resting, where user placed the phone firmly against his body, resulted in the highest and most consistent identification results as well as highest correlation coefficient in all evaluated cases.

With regard to standing or walking, sensor data generated from its resting state contained much lower variability, further boosting that of the correlation-based authentication model. These results indicate that reduced motion artifact and invariant device orientation can significantly enhance recognition accuracy. These results further highlight inter-user condition distinctions that call for integrating contextual awareness into smartphone-based authentication systems.

As a further step to enhance the reliability and effectiveness of behavioral authentication, the incorporation of supplementary data sources is suggested. These might be virtual sensors—inferred measures acquired from sensor fusion or machine learning-based estimators—that can reside on top of more delicate as well as steady behavioral patterns. These additions could result in richer user profiling and error rates lower due to fleeting behavioral variations.

According to these results, a student verification system was constructed applicable to teaching situations, especially to tele-teaching and online testing. This system gave a higher weighting to behavioral data recorded in resting situations when motion signals most stabilized and device stabilities most stabilized as user-subject specific. While motion and standing situations also yielded workable data results, higher variability in those situations resulted in lower authentication certainty.

As a whole, the results confirm that sensor placement as well as behavioral context play a significant role in developing secure and efficient user-friendly mobile-authentication systems. These findings have particular significance in online-class platforms, where ongoing and real user identification is necessary to preserve college/integrity and protect individual information.

Conclusion. This work proposed a behavioral-based model of smartphone users to enhance security in cognitively aware educational platforms. Utilizing motion sensor information, namely gyroscope and accelerometer measurements, the system allows context-aware verification to be performed at all times through individual patterns of interaction. Test results validated that proper device positioning, especially when resting, effectively

improved authentication correctness significantly, further supporting its application in mobile learning environments.

Notwithstanding its prospective performance, some implementation issues remain. These are protection of user privacy, providing ubiquity in differently behavioral contexts, and avoidance of vulnerability to spoofing or adverse manipulation. To enhance reliability as well as user acceptability, future work must look into a hybrid authentication system that integrates behavioral information with conventional credentials like passwords or biometric signatures.

Further maturation of behavioral authentication systems will be facilitated by growing the pool of compared features—such as gesture dynamics, input behavior, and usage patterns—as well as improving underlying algorithms to allow superior scalability and robustness. Incorporating real-time learning mechanisms could also facilitate improved personalization and adaptability to user-generic behavior with time.

Overall, behavioral authentication is a significant step towards safe and user-friendly learning systems. Addressing security measures to natural behavioral patterns, such patterns can facilitate data security as well as user activity and push forward trusted, efficient, as well as adaptive learning platforms online.

Funding. *This research has been/was/is funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. BR24993072).*

References

1. Schewina K. I., Clausen S., Basyurt A. S., Stieglitz S. Information privacy and user satisfaction in mobile applications: A cross-national analysis// International Conference on Information Systems (ICIS), AIS Electronic Library. -2024.

2. Kocsis D., Shepherd M., Segal D. L. Cyber hygiene training: Using a Salesforce developer module to improve student online behaviors//Journal of Information Systems Education. -2025. -Vol.36(2). -P.90-110. DOI 10.62273/CUEU6233.

3. Liébana-Cabanillas F., Kalinic Z., Muñoz-Leiva F., Higueras-Castillo E. Biometric m-payment systems: A multi-analytical approach to determining use intention//Information & Management. -2024. -Vol.61 (2): 103907. DOI 10.1016/j.im.2023.103907.

4. Sejjari A., Moujahdi C., Assad N., Haidine A. Dynamic authentication on mobile devices: Evaluating continuous identity verification through swiping gestures // Signal, Image and Video Processing. -2024. -Vol.18. -P.9095-9193. DOI 10.1007/s11760-024-03532-3.

5. Lim W.P., Ooi S.Y., Pang Y.H., Ramalingam S., Chew Y.J. Dynamic touchstroke analysis with explainable artificial intelligence tree-based learners // Journal of Telecommunications and the Digital Economy. -2024. -Vol.12(4). -P.137-161. DOI 10.18080/jtde.v12n4.1023.

6. Sağbaş E.A., Ballı S. Machine learning-based novel continuous authentication system using soft keyboard typing behavior and motion sensor data // Neural Computing and Applications. - 2024. -Vol.36. -P. 5433-3445. DOI 10.1007/s00521-023-09360-9.

7. Mekruksavanich S., Jitpattanakul A. Wearable sensor-based behavioral user authentication using a hybrid deep learning approach with squeeze-and-excitation mechanism//Computers. -2024. -Vol.13(12): 337. DOI 10.3390/computers13120337.

8. Alawami M.A., Abuhmed T., Abuhamad M., Kim H. MotionID: Towards practical behavioral biometrics-based implicit user authentication on smartphones // Pervasive and Mobile Computing. -2024. -Vol.83: 101922. DOI 10.1016/j.pmcj.2024.101922.

9. Kokal S., Vanamala M., Dave R. Analysis of gait motion sensor mobile authentication with machine learning // International Journal of Advanced Computer Science and Applications. -2024. -Vol.15(3): 9-15. DOI 10.14569/IJACSA.2024.0150302.

10. Cariello N., Levine S., Zhou G., Hoplight B., Gasti P. SMARTCOPE: Smartphone Change Of Possession Evaluation for continuous authentication // Pervasive and Mobile Computing. -2024. -Vol.97: 101873. DOI 10.1016/j.pmcj.2023.101873.

11. Li Y., Huang Y., Huang H. FuMeAuth: Sensor-based continuous authentication using fused memory-augmented transformer autoencoder//IEEE Internet of Things Journal. -2024. -Vol.11(15). -P. 26340-26351. DOI 10.1109/JIOT.2024.3394437.

12. Delgado-Santos P., Tolosana R., Guest R., Deravi F., Vera-Rodriguez R. Exploring transformers for behavioural biometrics: A case study in gait recognition // Pattern Recognition. - 2023. - Vol.143: 109798. DOI 10.1016/j.patcog.2023.109798.

13. Delgado-Santos P., Tolosana R., Guest R., Vera-Rodriguez R., Fierrez J. M-GaitFormer: Mobile biometric gait verification using Transformers // Engineering Applications of Artificial Intelligence. - 2023. -Vol. 125: 106682. DOI 10.1016/j.engappai.2023.106682.

14. Alotaibi B., Alotaibi M. Hybrid deep learning framework for continuous user authentication based on smartphone sensors // Sensors. -2025. -Vol.25(9): 2817. DOI 10.3390/s25092817.

15. Li Y., Liu L., Deng S., Qin H., El-Yacoubi M.A. Memory-augmented autoencoder-based continuous authentication on smartphones with conditional transformer GANs//IEEE Transactions on Mobile Computing. -2024. -Vol.23(5). -P.4467-4482. DOI 10.1109/TMC.2023.3290834.

16. Delgado-Santos P., Tolosana R., Guest R., Lamb P., Khmelnitsky A., et al. SwipeFormer: Transformers for mobile touchscreen biometrics // Expert Systems with Applications. -2024. -Vol.237(Part C): 121537. DOI 10.1016/j.eswa.2023.121537.

17. Shen Z., Li S., Zhao X., Zou J. IncreAuth: Incremental-learning-based behavioral biometric authentication on smartphones // IEEE Internet of Things Journal. -2024. -Vol.11(1). -P. 5674–5687. DOI 10.1109/JIOT.2023.3289935.

18. Yang Z., Li Y., Zhou G. Unsupervised sensor-based continuous authentication with low-rank transformer using learning-to-rank algorithms // IEEE Transactions on Mobile Computing. - 2024. - Vol.23(9). -P. 8839-8854. DOI 10.1109/TMC.2024.3353209.

19. Li Y., Ouyang C., Huang H. AEGANAuth: Autoencoder GAN-based continuous authentication with conditional variational autoencoder generative adversarial network // IEEE Internet of Things Journal. -2024. -Vol.11(16). -P.27635-27650. DOI 10.1109/JIOT.2024.3399549.

20. Nguyen K.-N., Rasnayaka S., Wickramanayake S., Meedeniya D., Saha S., Sim T. Spatio-Temporal Dual-Attention Transformer for Time-Series Behavioral Biometrics//IEEE Transactions on Biometrics, Behavior, and Identity Science. - 2024. -Vol.6(4). -P. 591-601. DOI 10.1109/TBIOM.2024.3394875.

21. Kumari S., Singh K., Khan T., Ariffin M. M., Mohan S. K., et al. A novel approach for continuous authentication of mobile users using reduce feature elimination (RFE): A machine learning approach // Mobile Networks and Applications. -2023. -Vol.28. -P.767–781. DOI 10.1007/s11036-023-02103-z.

22. Gunawardena N., Ginige J. A., Javadi B. Eye-tracking technologies in mobile devices using edge computing: A systematic review // ACM Computing Surveys. -2023. -Vol.55(8): 158. DOI 10.1145/3546938.

23. Nosrati L., Bidgoli A.M., Javadi H.H.S. Machine learning and metaheuristic algorithms for voice-based authentication: A mobile banking case study // International Journal of Computational Intelligence

Systems. -2024. -Vol.17: 287. DOI 10.1007/s44196-024-00690-7.

24. Cao H., Liu D., Jiang H., Cai C., Zheng T., Lui J.C.S. HandKey: Knocking-Triggered Robust Vibration Signature for Keyless Unlocking // IEEE Transactions on Mobile Computing. -2024. -Vol.23(1). -P.520-534. DOI 10.1109/TMC.2022.3216868.

25. Cao H., Jiang H., Yang K., Chen S., Wu W., et al. Data-Augmentation-Enabled Continuous User Authentication via Passive Vibration Response // IEEE Internet of Things Journal. -2023. -Vol.10(16). -P.14137–14151. DOI 10.1109/JIOT.2023.3264274.

26. Zhang J., Li Z., Zhang H., Zhang W., Ling Z., et al. Sensor-based implicit authentication through learning user physiological and behavioral characteristics // Computer Communications. -2023. -Vol.208(C). -P.244–255. DOI 10.1016/j.comcom.2023.06.016.

27. Chen F., Xin J., Phoha V.V. SSPRA: A robust approach to continuous authentication amidst real-world adversarial challenges // IEEE Transactions on Biometrics, Behavior, and Identity Science. -2024. -Vol.6 (2). -P.245-260. DOI 10.1109/TBIOM.2024.3369590.

28. Li X., Li R. A trustworthiness evaluation mechanism based on principles-assumptions model// IEEE Internet of Things Journal. -2024. -Vol.11(10). -P.17510-17524. DOI 10.1109/JIOT.2024.3357705.

Сведения об авторах

Сербин В.В. - кандидат технических наук, Ассоциированный профессор Satbayev University, Алматы, Казахстан, e-mail:v.serbin@satbayev.university;

Қасенхан А.М. - доктор Ph.D, Satbayev University, Алматы, Казахстан, e-mail: a.kassenkhan@satbayev.university;

Кальпеева Ж.Б. - доктор Ph.D, Satbayev University, Алматы, Казахстан, e-mail: z.kalpeyeva@satbayev.university;

Ускенбаева Р.К. - доктор технических наук, Профессор, Satbayev University, Алматы, Казахстан, e-mail: r.k.uskenbayeva@satbayev.university.

Information about the authors

Serbin V.V. - Candidate of Technical Sciences, Associate Professor, Satbayev University, Almaty, Kazakhstan, e-mail: v.serbin@satbayev.university;

Kassenkhan A.M. - PhD, Satbayev University, Almaty, Kazakhstan, e-mail: a.kassenkhan@satbayev.university;

Kalpeyeva Zh.B. - доктор PhD, Satbayev University, Almaty, Kazakhstan, e-mail: z.kalpeyeva@satbayev.university;

Uskenbayeva R.K. - Doctor of technical sciences, Professor, Satbayev University, Almaty, Kazakhstan, e-mail: r.k.uskenbayeva@satbayev.university.