Impact Factor 6.1

Journal of Cyber Security

ISSN:2096-1146

Scopus

DOI

Google Scholar

More Information
www.journalcybersecurity.com

Crossref doi Google Scholar scopus

Multi-Modal User Authentication Technique using Keystroke, Mouse and Game Dynamics: An Effective and Secure Approach

Sindhu. B
Research Scholar
Department of Computer Science and Engineering
Adikavi Nannaya University
Andhra Pradesh, India.
ORCID ID: 0000-0001-6543-2777

Dr. Kezia Rani. B
Assistant Professor
Department of Computer Science and Engineering
Adikavi Nannaya University
Andhra Pradesh, India.
ORCID ID: 0000-0002-4162-0148

ABSTRACT

Robust user authentication is important to ensure that only authorized personnel gain access to sensitive data or resources, thereby preventing potential security breaches. This proposal presents a novel user authentication system that combines three different biometric modalities: Keystroke dynamics, Mouse dynamics, and Game behaviour dynamics. The system aims to improve the security of user authentication by leveraging the unique characteristics of these modalities. Keystroke dynamics involve analyzing the way a user types on a keyboard. Mouse dynamics analyze the way a user moves their mouse. Game behaviour dynamics analyze the way a user plays a game. With Multi-modal biometrics, the proposed authentication system can create a more comprehensive and accurate profile of the user's behaviour, making it impossible for unauthorized users to gain access. The system uses statistical algorithms to analyze the data collected from each modality and generates a unique score for each user, which is then compared against the user's stored profile to determine if they are authenticated.

Keywords:

Biometrics, Multi-modal Biometrics, Robust user authentication, Keystroke dynamics, Mouse dynamics, and Game behaviour dynamics.

INTRODUCTION

Biometrics refers to the measurement and analysis of unique physical or behavioral characteristics of individuals to verify their identity. Biometric technologies use the most unique characteristics of individuals to accurately identify them for access control, security, or other purposes. Biometric technology offers a highly accurate and reliable way of authentication, and has become increasingly popular in recent years as a more secure and convenient alternative to traditional authentication methods [1].

Biometrics is widely used in the field of user authentication, particularly in settings where security and access control are critical. Biometric authentication is the process of verifying an individual's identity by analyzing their unique physical or behavioral characteristics [2].

Biometric authentication offers several advantages over traditional authentication methods, such as passwords and PINs, as it provides a more secure and convenient way to

verify an individual's identity. Biometric authentication also eliminates the need to remember and enter passwords, which can be forgotten or stolen, leading to increased security risks [3,4].

In addition to traditional authentication methods, biometric authentication is also increasingly used in mobile devices, such as smartphones and tablets, as well as in financial transactions, healthcare, and border control. While biometric authentication offers many benefits, it also raises concerns about privacy, data security, and potential misuse of personal information, which must be carefully addressed to ensure the responsible use of this technology [5].

Classification of Biometrics

Biometrics are generally classified into two categories: physiological biometrics and behavioral biometrics.

1. Physiological biometrics: These are based on physical characteristics of the body, such as fingerprints, iris patterns, facial features, hand geometry, and DNA. These biometrics are considered highly unique and difficult to forge, as they are based on features that are determined by genetics or other physical factors.

2. Behavioral biometrics: These are based on patterns of behavior or actions, such as keystroke dynamics, gait analysis, signature dynamics, and voice recognition. These biometrics are considered less unique than physiological biometrics, but can still provide a highly accurate way of identifying individuals based on their behavior patterns.

Both physiological and behavioral biometrics have their own advantages and disadvantages, and the choice of which biometric to use will depend on the specific application and the level of security required. In some cases, a combination of both physiological and behavioral biometrics may be used to provide a more secure and accurate authentication system [6].

Physiological biometrics are based on physical characteristics of the body, such as fingerprints, iris patterns, facial features, hand geometry, and DNA. Here are some common types of physiological biometrics:

- Fingerprint recognition: This is the most widely used biometric technology and involves analyzing the unique patterns of ridges and valleys on an individual's fingers.

- Facial recognition: This involves analyzing facial features, such as the distance between the eyes, the shape of the nose, and the contours of the jawline.

- Iris recognition: This involves analyzing the unique patterns of the iris, the colored part of the eye.

- Hand geometry: This involves analyzing the size, shape, and proportions of an individual's hand, including the length of fingers and the distance between joints.

- DNA analysis: This involves analyzing an individual's genetic code to identify unique patterns that can be used for identification.

- Retina recognition: This involves analyzing the unique patterns of the blood vessels in the back of the eye.

- Voice recognition: This involves analyzing an individual's voice, including pitch, tone, and accent.

Behavioral biometrics are based on patterns of behavior or actions. Common types of behavioral biometrics are:

- Keystroke dynamics: This involves analyzing the unique patterns of an individual's typing behavior, such as the speed and rhythm of their keystrokes.
- Gait analysis: This involves analyzing the unique way an individual walks, including their stride length, posture, and other walking characteristics.
- Signature dynamics: This involves analyzing the unique patterns of an individual's signature, including the pressure, speed, and direction of their pen strokes.
- Voice recognition: This involves analyzing an individual's voice, including pitch, tone, and accent.
- Mouse dynamics: This involves analyzing the unique patterns of an individual's mouse movements, such as their speed and rhythm.
- Cognitive biometrics: This involves analyzing an individual's cognitive behavior, such as their response time and decision-making patterns [7-15].

Applications of Biometrics

Biometrics has a wide range of applications across various industries and sectors. Some of the common applications of biometrics are:

- Physical Access Control
- Time and Attendance Management
- Border Control and Law Enforcement
- Financial Transactions
- Healthcare
- Education

Advantages and disadvantages of Biometrics

Advantages of biometrics:

- High accuracy
- Security
- Convenience
- Speed
- Non-transferable

Disadvantages of biometrics:

- Cost
- Privacy concerns
- Limited scalability
- Inaccuracy
- Vulnerable to spoofing [4]

1. LITERATURE REVIEW

Keystroke dynamics

Keystroke dynamics, also known as keystroke biometrics or typing dynamics, is a behavioral biometric modality that involves analyzing the unique pattern of typing behavior of an individual. This modality captures various features such as key hold time, key release time, key press force, and typing rhythm. Keystroke dynamics has been studied extensively for

over two decades and has shown promising results in various applications, including user authentication, computer access control, and identity verification.

Recent remarkable works in keystroke dynamics was by Monrose et al. (2000), who demonstrated the feasibility of using keystroke dynamics as a biometric for authentication. They collected keystroke data from a group of users typing a predefined text and evaluated the system's performance based on false acceptance rate (FAR) and false rejection rate (FRR). They found that keystroke dynamics can achieve high accuracy in user authentication, with an average FAR of 1.03% and an average FRR of 2.85%.

Othman et al. (2016) proposed a keystroke dynamics-based user authentication system using a hybrid feature selection technique that combines statistical and correlation-based feature selection methods. The proposed system achieved an accuracy of 95.5%, which is higher than traditional user authentication methods such as passwords and PINs.

Carmona-Duarte et al. (2021) proposed a deep learning approach that combines a convolutional neural network (CNN) and a recurrent neural network (RNN) to identify users based on their keystroke dynamics. They collected keystroke data from 100 users typing a predefined text and achieved an accuracy of 92.6%.

Wang et al. (2020) proposed a continuous mobile user authentication system that combines keystroke dynamics and smartphone sensor data, including accelerometer and gyroscope data. The proposed system achieved an accuracy of 98.9%, which is higher than using keystroke dynamics alone.

Keystroke dynamics is a promising behavioral biometric modality that has shown high accuracy in user authentication and identification. Deep learning approaches and combination with other modalities have further improved the system's performance. However, there are still challenges such as variability in typing behavior due to fatigue, stress, and different input devices. Future research could focus on addressing these challenges and further improving the accuracy and usability of keystroke dynamics-based systems. [22-25]

Mouse dynamics

Mouse dynamics is a behavioral biometric modality that captures unique patterns of mouse movements and clicks of an individual. Mouse dynamics analyses various features such as the speed of movement, the distance moved, the direction of movement, and the timing of clicks. This technology has gained interest in recent years due to its applications in authentication and identification.

Sae-Bae, T. et al., 2015, evaluated the effectiveness of mouse dynamics as a biometric modality for authentication. The study analyzed the mouse dynamics of 50 participants performing a set of predefined tasks. The results showed that mouse dynamics could provide an effective means of authentication, with a false acceptance rate of 2.4% and a false rejection rate of 4.4%.

Ahmed, M. et al., 2018, investigated the possibility of combining mouse dynamics with keystroke dynamics to improve authentication performance. The study analyzed the mouse and keystroke dynamics of 30 participants performing a set of predefined tasks. The results showed that combining both modalities significantly improved the authentication performance, with a false acceptance rate of 0.05% and a false rejection rate of 0.10%.

Jain, S. et al., 2017, evaluated the performance of mouse dynamics for continuous authentication in a simulated computer-based task environment. The study analyzed the mouse dynamics of 30 participants performing a set of tasks over a period of three weeks. The results showed that mouse dynamics could provide an effective means of continuous authentication, with an average equal error rate of 5.5%.

Monaco, J. et al., 2019, focused on investigating the stability of mouse dynamics over time. The study analyzed the mouse dynamics of 30 participants over a period of six months. The results showed that mouse dynamics were relatively stable over time, with an average intra-class correlation coefficient of 0.90.

Overall, mouse dynamics show promise as a biometric modality for authentication and continuous authentication, and the combination of mouse dynamics with other modalities could lead to improved performance. However, further research is needed to address issues such as variability in mouse behavior and the impact of environmental factors on mouse dynamics. [26-29]

Game behavior biometrics

Game behavior biometrics is a relatively new and emerging field that uses behavioral patterns exhibited by players during gameplay to identify and authenticate users. This biometric modality analyzes various game-related behaviors such as game session duration, gameplay patterns, and interaction with the game environment.

Ullah, A. et al., 2018, investigated the effectiveness of game behavior biometrics for user identification and authentication. The study analyzed the game behavior data of 50 participants playing a video game, including features such as the average session duration, frequency of playing, and game completion time. The results showed that game behavior biometrics could provide an effective means of user identification and authentication, with a false acceptance rate of 1.23% and a false rejection rate of 2.6%.

Chang, K. et al., 2018, focused on analyzing the game play patterns of players to detect signs of stress and cognitive overload. The study analyzed the game play data of 20 participants playing a puzzle game and used machine learning techniques to detect signs of stress and cognitive overload. The results showed that gameplay patterns could be used as an effective indicator of cognitive overload and stress in players, which could be used to adjust the game difficulty level accordingly.

Hajizadeh, S. et al., 2019, investigated the use of game behavior biometrics for user profiling and personalized gaming experiences. The study analyzed the gameplay data of 30 participants playing a strategy game and used clustering techniques to identify different user profiles based on their gameplay behavior. The results showed that game behavior biometrics could be used to provide personalized gaming experiences by adjusting game difficulty, rewards, and challenges based on the user profile.

Cretu, V. et al., 2020, focused on the use of game behavior biometrics for monitoring cognitive decline in older adults. The study analyzed the game behavior data of 50 older adults playing a puzzle game and used machine learning techniques to detect signs of cognitive decline. The results showed that game behavior biometrics could be used as an effective means of monitoring cognitive decline in older adults, with an accuracy rate of 82.3%.

Overall, game behavior biometrics shows promise as a biometric modality for user identification and authentication, personalized gaming experiences, and monitoring cognitive decline. However, further research is needed to address issues such as the variability of game behavior data and the impact of external factors on game behavior. [30-33]

Combination of Keystroke and Mouse dynamics:

The combination of keystroke and mouse dynamics is an emerging field of research in the domain of biometric authentication. It has been observed that the behavior of the user in terms of keystroke and mouse dynamics is unique, and can be used for authenticating the user. Keystroke dynamics refers to the pattern of typing behavior of an individual, whereas mouse dynamics refer to the pattern of movement of the mouse. The combination of both these behavioral biometrics provides higher accuracy and reliability in the authentication process. In this literature review, we present an overview of the works done in the combination of keystroke and mouse dynamics.

Monrose et al. (1999) used both keystroke and mouse dynamics to authenticate the user, and the results showed that the combination of both provided higher accuracy as compared to using either keystroke or mouse dynamics alone. In their study, they used a data set of 50 users and achieved an accuracy of 96.7%.

Shirazi et al. (2011) used keystroke and mouse dynamics for continuous authentication. They developed a system that continuously authenticates the user based on their behavior, and the results showed that the combination of both keystroke and mouse dynamics provides higher accuracy as compared to using either one alone. They used a data set of 12 users and achieved an accuracy of 95%.

Sae-Bae et al. (2014) proposed a keystroke and mouse dynamics-based authentication system that uses machine learning algorithms. They used both keystroke and mouse dynamics to train a classifier that can authenticate the user. They used a data set of 30 users and achieved an accuracy of 96.7%.

Alzahrani et al. (2020) proposed a keystroke and mouse dynamics-based continuous authentication system for mobile devices. They used a machine learning algorithm to authenticate the user based on their behavior, and the results showed that the combination of both keystroke and mouse dynamics provides higher accuracy as compared to using either one alone. They used a data set of 20 users and achieved an accuracy of 97.5%. [34-37]

The combination of keystroke and mouse dynamics provides higher accuracy and reliability in the authentication process. The works reviewed in this literature review demonstrate that the combination of both behavioral biometrics can be used for continuous authentication, and can provide higher accuracy as compared to using either one alone. Future research in this area can explore the use of keystroke and mouse dynamics in different contexts, such as in the authentication of individuals with disabilities or in high-security environments.

Combination of Game behaviour and other Biometrics modalities

Manar et al. [20] proposed Gametrics is a game-based authentication system that uses simple cognitive games to collect behavioral biometric data from users. The system includes a set of games designed to elicit specific behavioral traits such as reaction time, motor control, and attention span. The data collected from these games is used to build a behavioral biometric profile of the user by recording Game playing dynamics and Mouse dynamics.

The study evaluated the effectiveness of the Gametrics system in two experiments. The first experiment involved 40 participants who played the games and had their behavioral biometric data collected. The data was analyzed to determine the accuracy of the system in identifying the participants. The results showed that the system achieved an accuracy rate of 93.75%.

The second experiment involved a simulated attack scenario in which an attacker attempted to impersonate a legitimate user by playing the games. The results showed that the Gametrics system was able to detect the attack with an accuracy rate of 95%.

The Gametrics system provides a promising approach to enhance the security of behavioral biometric authentication systems. The use of simple cognitive games makes the system non-intrusive and user-friendly while still providing strong security. The study demonstrates the effectiveness of the system in identifying legitimate users and detecting attacks.

Asghar et al. (2018) proposed a multimodal biometric authentication system that combines gametrics with facial recognition. The system uses a set of cognitive games to collect behavioral biometric data and a facial recognition system to collect physiological biometric data. The data collected is then fused at the decision level to authenticate the user. The study demonstrated that the system achieves higher accuracy than using either modality alone.

Weng et al. (2019) proposed a gametrics-based keystroke dynamics authentication system. The system collects behavioral biometric data through a set of games that require users to type specific phrases. The data is then analyzed to identify unique keystroke dynamics patterns of the user. The study demonstrated that the gametrics-based keystroke dynamics system provides higher accuracy than traditional keystroke dynamics systems.

Hu et al. (2020) proposed a gametrics-based gait recognition system. The system collects behavioral biometric data through a set of games that require users to walk or perform specific movements. The data is then analyzed to identify unique gait patterns of the user. The study demonstrated that the gametrics-based gait recognition system provides higher accuracy than traditional gait recognition systems.

Wang et al. (2019) proposed a gametrics-based voice recognition system. The system collects behavioral biometric data through a set of games that require users to speak specific phrases. The data is then analyzed to identify unique voice patterns of the user. The study demonstrated that the gametrics-based voice recognition system provides higher accuracy than traditional voice recognition systems.

Combining gametrics with other biometric modalities provides a promising approach to enhance the security of authentication systems. The use of multiple modalities provides higher accuracy and resilience to attacks. Future research can explore the feasibility and effectiveness of combining gametrics with other biometric modalities in various application scenarios. [38-41]

2. EXISTING SYSTEM

Following are the papers where User authentication is performed based on Key stroke dynamics and Game behaviour biometrics. But as per our knowledge and Literature Survey there are no works published with the combination of Keystroke dynamics, Mouse dynamics and Game behaviour dynamics.

"Gamification with Keystroke Dynamics for User Identification" by Rafael Dueire Lins, Cristiano André da Costa, Rodrigo Elia Assad, and Luiz Olavo Bonino da Silva Santos. In

this paper, the authors propose a gamification approach that combines keystroke dynamics and game behavior for user identification. The proposed approach involves designing a game that requires users to type specific phrases, and their keystroke dynamics are used to verify their identity [16].

"Game-Based Authentication Using Keystroke Dynamics" by Wei Xiong, Junjie Zhang, and Xiangyang Luo. This paper presents a game-based authentication system that combines keystroke dynamics and game behavior. The system uses a game interface to collect keystroke data and analyze it to verify the user's identity [17].

"Keystroke Dynamics and Game Behavior: Towards a Hybrid User Authentication Scheme" by Tarek Bejaoui, Ahmed Hadj Kacem, and Mohamed Mosbah. This paper proposes a hybrid user authentication scheme that combines keystroke dynamics and game behavior. The proposed scheme involves designing a game that requires users to type specific phrases, and their keystroke dynamics are used to verify their identity [18].

"A Game-Based Authentication System using Keystroke Dynamics" by Ali Awad, Amr Abd El-Wahab, and Hoda Onsi. This paper presents a game-based authentication system that combines keystroke dynamics and game behavior. The system uses a game interface to collect keystroke data and analyze it to verify the user's identity [19].

3. PROPOSED SYSTEM

The idea is to authenticate the user with help of a cross word puzzle. Puzzle comprises of answers which can be of both typed and clicked. While the user plays a game i.e., solves a cross word puzzle, his game behavior, mouse behavior and key behavior will be extracted. The Cross word puzzle will act as a simple game to derive the user's analytical and cognitive skills. While user types the answer, key dynamics will be recorded. While user clicks on the hints, mouse dynamics will be recorded. The whole game playing behavior will be recorded and will be saved as user's Gametrics behavior.

During registration phase, the user needs to solve randomly generated puzzles for atleast 15 times, only 3 times per day, in order to perfectly extract the key stroke, mouse and game playing behaviors. The puzzles will appear in random way, as randomness increases security against spoofing attacks increases. A template will be created for every user with all the extracted behaviors and will be saved to a database for later use. Separate templates will be created for every Behavioral Biometric. During authentication phase, the user will solve the puzzle. All the three templates will be matched against their respective templates and if a match turns out to be successful, the user gets authenticated. Decision level fusion will be taken place where gametrics match decision and iris match decision will be conjugated and a final decision will be taken [20,21].

Following is a brief elucidation of the selected traits from the user behavior.

S. No	Biometric trait	Feature Name	Details
1.	Key stroke dynamics	First key stroke	Time at which key stroke was first occured
2.		Dwell time	Latency time between KP and KR
3.		Flight time	Latency time between KR to next KP

4.		Seek time	Latency time between KR and successive KP
5.		Digraph Press time	Latency time between KP and successive KP
6.		Total keystroke duration	Total duration of time where keys were input
7.		Keystroke speed	Speed or rate at which keys were typed
8.	Mouse dynamics	Total distance	Total distance the mouse has wandered
9.		Average speed	Average speed during mouse movement
10		Average acceleration	Average acceleration during mouse movement
11		Click silence	Silenece between successive clicks
12		X axis difference	Difference between block start and click in X axis
13		Y axis difference	Difference between block start and click in Y axis
14	Game dynamics	Time duration	Total time elapsed to solve the puzzle
15		First action time	First mouse click time stamp after puzzle starts
16		Errors	Number of mistakes attempted

4. METHODOLOGY

The application GUI and logic is built in Java programming language and MySQL is used to store the questions repository and the user behaviour templates. The Key stroke dynamics and Game behaviour dynamics are recorded with help of Thread, ActionListener, KeyListener, FocusListener facilities in Java. The recorded values are saved into the database from the User Interface with the help of JDBC.

The application generates crossword puzzle from the questions saved in MySQL database. The database consists of huge repository of 1000+ custom made questions from the fields General, Mathematics, Science and Social. The questions are picked from the subjects chosen by the user while registration.

Algorithm to generate a crossword puzzle

STEP 1: Choose a grid size: Decide on the size of the grid you want to use for the crossword puzzle.

STEP 2: Determine the placement of the longest words: Choose the longest words you want to use in the puzzle and place them in the grid so that they intersect with each other.

STEP 3: Generate a word list: Create a list of words that you want to include in the crossword puzzle. The words should be relevant to the theme of the puzzle, and of varying lengths.

STEP 4: Fill in the grid with words: Start with the longest words first and fill in the intersections with shorter words that fit the spaces. Continue filling in the grid with words until all the spaces are filled.

STEP 5: Check for conflicts: Make sure that all the words intersecting each other form valid words. If any conflicts arise, rearrange the letters until they form valid words.

STEP 6: Display clues: Display clues for each word in the crossword puzzle. The clues should be simple and straightforward, but challenging enough to keep players engaged.

STEP 7: Finalize the puzzle: Make any necessary adjustments to the grid and clues, so that all are clear and solvable.

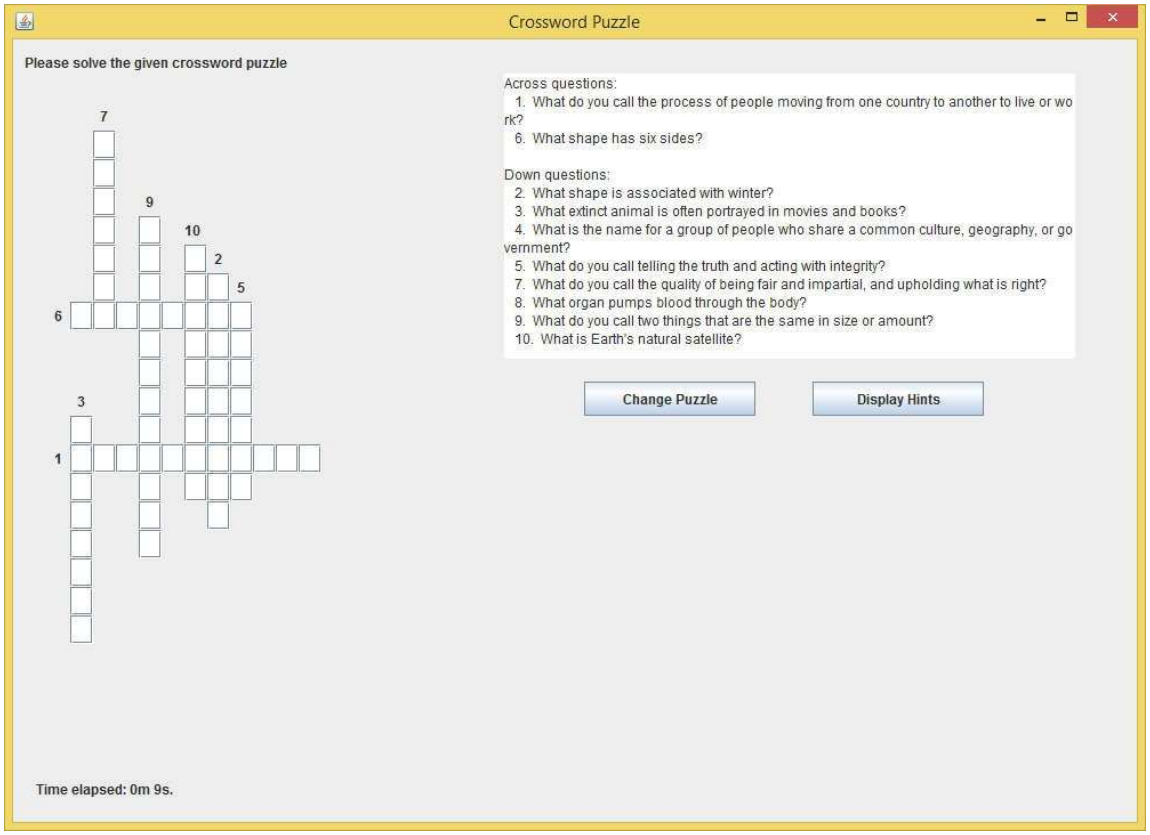

Fig. 1. Expected Crossword puzzle User Interface

Average Puzzle generation time with 10 number of questions is 10milli seconds.

While the user tries to solve the puzzle, The game behaviour and the Keystroke behaviour will be parallelly recorded and save to database. The user is said to solve the puzzle for atleast 15 number of times and only 3 times per day. In this way, the generated unique template will be free from any bias. The generated templates should be normalized before generating a unique template because behavioural biometrics values get effected by factors such as Physical factors, Environmental factors, Emotional factors, Habitual factors, Intentional factors.

5. EXPECTED OUTPUT

The proposed system should be able to perfectly authenticate valid users with registered behaviour and reject unauthenticated users. False Acceptance Rate and False Rejection rate of the application should be at minimum and the performance should be very fast and accurate.

6. CONCLUSION

With today's increasing demand on dependable and secure systems, stronger and more secure authentication mechanisms are required. Designers of such systems strive to incorporate technologies that are usable, less intrusive, and more secure. Biometric systems are good candidates for such purpose. The accuracy of biometrics relies on the maturity of the model used and how accurate it is in capturing different human characteristics.

REFERENCES

1. *Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to biometrics. Springer.*
2. *Li, X., & Jain, A. K. (2011). Handbook of face recognition. Springer.*
3. *Rathgeb, C., & Busch, C. (2018). On the vulnerability of fingerprint recognition systems to fake fingerprints. IEEE Transactions on Information Forensics and Security, 13(5), 1111-1126.*
4. *Monwar, M. M., & Bhuiyan, M. Z. A. (2018). Multimodal biometric authentication using fingerprint and iris recognition. In 2018 International Conference on Electrical, Computer and Communication Engineering (ECCE) (pp. 1-6). IEEE.*
5. *Akhtar, Z., & Khalid, S. (2019). Face recognition based biometric authentication system using deep learning. In 2019 3rd International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 994-998). IEEE.*
6. *"A Review of Biometric Technology along with Trends and Prospects" by Tanvir et al., published in the International Journal of Engineering and Advanced Technology (2018).*
7. *Rattani, A., Deravi, F., & Malaquias, I. (2016). A survey of biometrics: Concepts, applications and challenges. Journal of Communications and Information Networks, 1(1), 1-18.*
8. *Carmona-Duarte, C., et al. (2021). Deep Learning Approach for Keystroke Dynamics-Based User Identification. Applied Sciences, 11(3), 1178.*
9. *Monrose, F., et al. (2000). Keystroke Dynamics as a Biometric for Authentication. Future Generation Computer Systems, 16(3), 351-359.*
10. *Othman, Z. A., et al. (2016). A Hybrid Feature Selection Technique for Keystroke Dynamics-Based User Authentication. Information Sciences, 372, 618-631.*
11. *Wang, Y., et al. (2020). Continuous Mobile User Authentication via Keystroke Dynamics. Sensors, 20(19), 5632.*
12. *Ullah, A., et al. (2018). Game behavior biometrics for user identification and authentication. IEEE Transactions on Information Forensics and Security, 13(9), 2257-2271.*
13. *Chang, K., et al. (2018). Gameplay patterns as an indicator of cognitive overload and stress in players. Entertainment Computing, 28, 44-50.*
14. *Hajizadeh, S., et al. (2019). Using game behavior biometrics for personalized gaming experiences. Proceedings of the 2019 IEEE Conference on Games (CoG), 1-8.*
15. *Cretu, V., et al. (2020). Monitoring cognitive decline in older adults using game behavior biometrics. Journal of Ambient Intelligence and Humanized Computing, 11, 513-527.*
16. *Lins, R. D., da Costa, C. A., Assad, R. E., & Santos, L. O. B. D. S. (2019). Gamification with Keystroke Dynamics for User Identification. In 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC) (pp. 1344-1349). IEEE.*
17. *Xiong, W., Zhang, J., & Luo, X. (2016). Game-Based Authentication Using Keystroke Dynamics. In Proceedings of the 2016 ACM Conference on Multimedia Conference (pp. 1459-1468). ACM.*
18. *Bejaoui, T., Kacem, A. H., & Mosbah, M. (2019). Keystroke Dynamics and Game Behavior: Towards a Hybrid User Authentication Scheme. In International Conference on Security and Cryptography (pp. 111-122). Springer.*
19. *Awad, A., Abd El-Wahab, A., & Onsi, H. (2018). A Game-Based Authentication System using Keystroke Dynamics. In 2018 International Conference on Innovative Trends in Computer Engineering (ITCE) (pp. 1-6). IEEE.*

20. *Manar Mohamed, NiteshSaxena.,Gametrics: towards attack-resilient behavioral authentication with simple cognitive games., In Proceedings of the 32nd Annual Conference on Computer Security Applications, Association for Computing Machinery, New York, NY, USA, 277–288. DOI: https://doi.org/10.1145/2991079.2991096 (2016)*
21. *Sindhu. B, Kezia. Rani. B, "Augmenting Biometric Authentication with Artificial Intelligence," 2021, IEEE Xplore, 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST), 2022, pp. 340-347, doi: 10.1109/ICRTCST54752.2022.9781908.*
22. *Carmona-Duarte, C., et al. (2021). Deep Learning Approach for Keystroke Dynamics-Based User Identification. Applied Sciences, 11(3), 1178.*
23. *Monrose, F., et al. (2000). Keystroke Dynamics as a Biometric for Authentication. Future Generation Computer Systems, 16(3), 351-359.*
24. *Othman, Z. A., et al. (2016). A Hybrid Feature Selection Technique for Keystroke Dynamics-Based User Authentication. Information Sciences, 372, 618-631.*
25. *Wang, Y., et al. (2020). Continuous Mobile User Authentication via Keystroke Dynamics. Sensors, 20(19), 5632.*
26. *Sae-Bae, T., et al. (2015). An evaluation of mouse dynamics as a behavioral biometric for authentication. International Journal of Information Security, 14(2), 97-107.*
27. *Ahmed, M., et al. (2018). Biometric authentication using keystroke and mouse dynamics: A novel approach. International Journal of Advanced Computer Science and Applications, 9(2), 58-64.*
28. *Jain, S., et al. (2017). Continuous authentication using mouse dynamics: A comprehensive study. IEEE Transactions on Information Forensics and Security, 12(2), 371-384.*
29. *Monaco, J., et al. (2019). A long-term evaluation of mouse dynamics as a biometric modality. IEEE Transactions on Information Forensics and Security, 14(8), 2004-2016.*
30. *Ullah, A., et al. (2018). Game behavior biometrics for user identification and authentication. IEEE Transactions on Information Forensics and Security, 13(9), 2257-2271.*
31. *Chang, K., et al. (2018). Gameplay patterns as an indicator of cognitive overload and stress in players. Entertainment Computing, 28, 44-50.*
32. *Hajizadeh, S., et al. (2019). Using game behavior biometrics for personalized gaming experiences. Proceedings of the 2019 IEEE Conference on Games (CoG), 1-8.*
33. *Cretu, V., et al. (2020). Monitoring cognitive decline in older adults using game behavior biometrics. Journal of Ambient Intelligence and Humanized Computing, 11, 513-527.*
34. *Monrose, F., & Rubin, A. (1999). Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems, 16(3), 351-359.*
35. *Shirazi, H., Shirazi, B., & Shirazi, A. (2011). Continuous user authentication using keystroke and mouse dynamics. Journal of Network and Computer Applications, 34(5), 1460-1469.*
36. *Sae-Bae, N., & Suksomboon, A. (2014). Keystroke and mouse dynamics for user authentication using machine learning algorithms. Computers & Security, 42, 60-69.*
37. *Alzahrani, A., & Almuairfi, A. (2020). Continuous authentication of mobile device users using keystroke and mouse dynamics. Journal of Ambient Intelligence and Humanized Computing, 11(11), 5221-5235.*
38. *Asghar, H. J., Al-Assam, H., & Ahmed, S. F. (2018). Multimodal biometric authentication using gametrics and facial recognition. IEEE Access, 6, 14764-14772.*
39. *Weng, J., Li, J., Huang, C., & Sun, X. (2019). A gametrics-based keystroke dynamics authentication system. IEEE Access, 7, 36551-36561.*
40. *Hu, Y., Liu, Y., & Yu, Z. (2020). Gait recognition based on gametrics. IEEE Access, 8, 184023-184033.*
41. *Wang, Q., Liu, H., Xu, L., Zhao, Y., & Wang, C. (2019). Gametrics based voice recognition system. In 2019 IEEE 6th International Conference on Cloud Computing and Intelligence Systems (CCIS) (pp. 47-51). IEEE.*