International Journal for Modern Trends in Science and Technology, 9(04): 381-390, 2023

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0904056
Available online at: http://www.ijmtst.com/vol9issue04.html

Novel Multi-Biometric Authentication System Based on Keystroke, Mouse and Game Behavior for High-Security Applications

Sindhu. B[1] | Dr. Kezia Rani. B[2]

[1]Research Scholar, Department of Computer Science and Engineering, Adikavi Nannaya University, Andhra Pradesh, India
sindhubangaru11@gmail.com, ORCID ID: 0000-0001-6543-2777
[2]Associate Professor, HOD, Department of Computer Science and Engineering, Adikavi Nannaya University, Andhra Pradesh, India
kezia.cse@aknu.edu.in, ORCID ID: 0000-0002-4162-0148

To Cite this Article
Sindhu. B and Dr. Kezia Rani. B. Novel Multi-Biometric Authentication System Based on Keystroke, Mouse and Game Behavior for High-Security Applications. International Journal for Modern Trends in Science and Technology 2023, 9(04), pp. 381-390. https://doi.org/10.46501/IJMTST0904056

Article Info
Received: 19 March 2023; Accepted: 20 April 2023; Published: 23 April 2023.

ABSTRACT

This paper presents a biometric authentication system based on keystroke, mouse, and game behavior. The system utilizes behavioral biometrics to provide a high level of security and usability in user authentication. By tracking user behavior across multiple biometric features, including keystroke dynamics, mouse dynamics, and game behavior, the system can generate a unique behavioral profile for each user, which can be used to authenticate the user with high accuracy. The system has numerous potential applications in various contexts, including finance, healthcare, military and government, e-commerce, online gaming, and social media. The system has been designed to be efficient and effective, with dynamic cross word puzzles generated in an average of 9ms and user authentication completed in 2ms. Overall, the biometric authentication system based on keystroke, mouse, and game behavior represents an exciting development in the field of biometric authentication, with significant potential to improve security and usability in a variety of contexts.

Keywords: Biometric authentication, Game behaviour dynamics, Behavioural biometrics, Keystroke dynamics, Mouse dynamics

1. INTRODUCTION

Biometrics is a technology that involves the measurement and analysis of biological characteristics or traits of an individual. These traits can be used to identify and verify the identity of an individual. Biometric authentication is becoming increasingly popular in many industries, including security, healthcare, banking, and law enforcement.

Biometric traits can be broadly categorized into two types: physiological and behavioral. Physiological traits include features such as fingerprint patterns, facial features, iris patterns, and DNA, while behavioral traits include aspects such as Keystroke dynamics, mouse dynamics, game behaviour, gait, voice and signature.

Biometric systems typically involve capturing an individual's biometric data through a sensor, which then processes the data and compares it with stored biometric data in a database to verify the individual's identity. Biometric technology is considered more secure than traditional authentication methods like passwords or

tokens, as biometric traits are unique to an individual and difficult to fake or steal.

However, biometric technology also raises concerns about privacy, data protection, and the potential for misuse of personal data. As such, the use of biometric technology is subject to strict regulations and guidelines to ensure its ethical and responsible use [1].

History of Biometrics

The history of biometrics dates back to ancient times, where humans have been using physical characteristics to identify individuals. For example, the Babylonians used fingerprints on clay tablets for business transactions, while the ancient Chinese used handprints to mark children's palm-prints in order to identify them later.

In the late 1800s, Sir Francis Galton, a cousin of Charles Darwin, conducted experiments on fingerprints and proposed their use for identification purposes. In 1892, Sir Edward Henry, a British police official, introduced fingerprinting as a means of identifying criminals, which quickly became a popular method of identification in law enforcement agencies around the world. The early 1900s saw the development of other biometric technologies, such as facial recognition, iris recognition, and voice recognition. In the mid-20th century, advances in computer technology allowed for more sophisticated biometric systems to be developed.

Since then, biometric technology has continued to evolve and become more accurate and reliable, with new modalities such as DNA analysis and vein recognition being developed. Today, biometric technology is used in a wide range of applications, including law enforcement, border control, financial services, healthcare, and access control. [2, 3]

Advancement of Biometric Technologies

Biometric technology has seen significant advancements in recent years, which has led to improved accuracy, speed, and ease of use. Here are some of the notable advances in biometric technologies:

1. Multi-modal biometrics: This refers to the use of multiple biometric modalities for identification, such as combining face and voice recognition or iris and fingerprint recognition. Multi-modal biometrics can improve accuracy and reduce the risk of false positives or false negatives.
2. Deep learning: Deep learning algorithms have been applied to biometric systems, allowing for more accurate and efficient recognition of biometric traits. These algorithms can learn and adapt to new data, making them more reliable and robust.
3. Mobile biometrics: The widespread use of smartphones has led to the development of mobile biometric systems, allowing for easy and convenient biometric authentication on mobile devices. This includes features such as facial recognition and fingerprint sensors on smartphones.
4. Contactless biometrics: The COVID-19 pandemic has accelerated the development of contactless biometric systems, which reduce the need for physical contact with biometric sensors. Examples include facial recognition and vein recognition systems.
5. Anti-spoofing techniques: To prevent biometric spoofing or presentation attacks, new anti-spoofing techniques have been developed, such as liveness detection and 3D face recognition.

These advancements have led to the widespread adoption of biometric technology in various industries and applications, improving security and convenience for users. [4-6]. Advancements in User authentication techniques are discussed in [18]

Applications of Biometrics

- Physical Access Control: Biometrics can be used for physical access control to secure areas such as government buildings, data centers, and corporate offices.
- Time and Attendance Management: Biometrics can be used for time and attendance management to track employees' working hours, breaks, and leaves accurately. This can improve productivity and reduce payroll errors.
- Border Control and Law Enforcement: Biometrics can be used for border control and law enforcement to identify and track criminals, terrorists, and unauthorized individuals. It can also be used for identification and verification at airports, seaports, and other entry points.

- Financial Transactions: Biometrics can be used for secure financial transactions, such as online banking, e-commerce, and mobile payments. It can enhance security and prevent fraud by verifying the identity of the user.
- Healthcare: Biometrics can be used in healthcare for patient identification and verification, drug dispensation, and medical record management. It can improve patient safety and reduce medical errors.
- Education: Biometrics can be used in education for student identification and verification, attendance tracking, and examination security. It can also be used for secure access to educational resources and facilities [7].

Advantages and disadvantages of Biometrics

Advantages of biometrics:

- High accuracy: Biometrics provides high accuracy in identifying and verifying individuals, as each person has unique physiological or behavioral traits.
- Security: Biometrics can enhance security and reduce fraud and identity theft.
- Convenience: Biometrics can provide a convenient and efficient way for individuals to authenticate themselves without the need for passwords or other traditional authentication methods.
- Speed: Biometric authentication can be fast and can reduce waiting times in high-traffic areas such as airports, stadiums, and other public places.
- Non-transferable: Biometric traits cannot be transferred or stolen, making it difficult for someone to impersonate another person.

Disadvantages of biometrics:

- Cost: Implementing biometric systems can be costly, especially for large organizations and institutions.
- Privacy concerns: Biometrics require collecting and storing personal and sensitive data, which can raise privacy concerns.
- Limited scalability: Some biometric systems may not be scalable, meaning they may not be able to handle a large number of users.
- Inaccuracy: Some biometric systems may not be 100% accurate and may generate false negatives or false positives, which can lead to inconvenience and errors.
- Vulnerable to spoofing: Some biometric systems may be vulnerable to spoofing or hacking, where someone may try to manipulate the system by using fake or modified biometric data [8]

Metrics to evaluate performance of Biometric systems

Following are the metrics that assess the performance of a specific biometric when implemented for authenticating users.

FTE- Failure To Enroll- refers to the percentage of population who have been unsuccessful during enrollment even after multiple attempts.

FTA- Failure To Acquire- refers to the probability of authentication system failure to acquire biometric data from the user even when the user's biometric is presented.

FAR- False Acceptance Rate- refers the probability of authentication system matching input sample to an incorrect template i.e., accepting invalid user. Can also be represented as

$$FAR = \frac{Number\ of\ invalid\ acceptances}{Total\ number\ of\ entries} * 100$$

FRR- False Rejection Rate- refers the probability of authentication system mismatching input sample to correct template i.e., rejecting valid user [1,18].

$$FRR = \frac{Number\ of\ valid\ rejections}{Total\ number\ of\ entries} * 100$$

2. LITERATURE REVIEW

Keystroke Dynamics

Keystroke dynamics is a biometric authentication method that identifies individuals based on their typing rhythm or keystroke patterns. The technique uses the time intervals between keystrokes and the duration of key press to create a unique profile of an individual's typing behavior. Here are some recent studies that have investigated the effectiveness of keystroke dynamics for biometric authentication [19].

In a study by Nguyen et al. (2021), the authors evaluated the performance of keystroke dynamics for continuous user authentication. The study used data collected from 57 participants typing a predefined set of sentences. The results showed that keystroke dynamics achieved an Equal Error Rate (EER) of 7.64%, indicating high accuracy in continuous user authentication. [9]

A study by Li et al. (2020) investigated the feasibility of keystroke dynamics as a secondary authentication mechanism for mobile devices. The authors used data collected from 50 participants typing a set of predefined phrases on a mobile phone. The study showed that keystroke dynamics could achieve an EER of 8.97%, indicating high accuracy in mobile authentication. [10]

In another study by Liu et al. (2019), the authors proposed a keystroke dynamics-based authentication method. The study used data collected from 50 participants typing a predefined set of sentences on a smartphone. The results showed that the proposed method achieved an EER of 7.2%, demonstrating high accuracy in smartphone authentication. [11]

Mouse movement dynamics

Mouse dynamics is a biometric authentication method that utilizes the movements and patterns of a computer mouse to create a unique profile of an individual's behavior. The technique uses the characteristics of mouse movements, such as speed, acceleration, and direction, to authenticate users. Here are some recent studies that have investigated the effectiveness of mouse dynamics for biometric authentication.

In a study by Karimian and Faez (2021), the authors proposed a novel mouse dynamics-based biometric authentication system that combines mouse movement features with keystroke dynamics. The study used data collected from 40 participants performing a set of predefined tasks. The results showed that the proposed system achieved an EER of 2.57%, indicating high accuracy in user authentication. [12]

In another study by Khalid et al. (2018), the authors proposed a mouse dynamics-based authentication system for mobile devices. The study used data collected from 20 participants performing various tasks on a mobile device. The results showed that the proposed system achieved an EER of 4.4%, indicating high accuracy in mobile device authentication. [13]

A study by Faez et al. (2018) investigated the effectiveness of mouse dynamics for user authentication in a continuous authentication setting. The study used data collected from 20 participants performing a set of predefined tasks. The results showed that mouse dynamics achieved an EER of 2.35%, indicating high accuracy in continuous user authentication. [14]

These studies demonstrate the potential of mouse dynamics as an effective biometric authentication method, particularly in mobile device security and continuous user authentication settings.

Game behaviour dynamics

Game behavior dynamics refer to the patterns and trends of player behavior within digital games. Analyzing and understanding game behavior dynamics can help game developers create more engaging and enjoyable games, as well as improve game security and prevent cheating. Here are some recent studies that have investigated game behavior dynamics:

In a study by Gao et al. (2020), the authors proposed a framework for analyzing player behavior dynamics in multiplayer online battle arena (MOBA) games. The study analyzed data collected from over 40,000 players of the popular MOBA game League of Legends. The results showed that the proposed framework was effective in identifying patterns of player behavior, such as preferred roles and strategies, as well as predicting player performance. [15]

In another study by Tang et al. (2021), the authors investigated the behavior dynamics of players in a popular multiplayer online role-playing game (MMORPG), World of Warcraft. The study analyzed data collected from over 50,000 players and identified several patterns of player behavior, such as quest completion and social interaction. The results also showed that player behavior dynamics could be used to predict player churn, or when players stop playing the game. [16]

A study by Tseng et al. (2018) investigated the potential of using game behavior dynamics as a biometric authentication method. The study analyzed data collected from players of the game Dota 2 and identified unique patterns of player behavior. The results showed that game behavior dynamics achieved an EER of 4.45%, indicating potential for use in biometric authentication. [17]

Overall, these studies demonstrate the potential of game behavior dynamics as a tool for understanding player behavior and improving game design, as well as its potential use in biometric authentication.

3. EXISTING SYSTEM

To the best of our knowledge and the extent of conducted Literature survey, there is currently no application available that combines the features of keystroke dynamics, mouse dynamics, and game behavior dynamics into a single system. While there have been many studies conducted on each of these individual features, the potential benefits of combining them have yet to be fully explored.

4. PROPOSED SYSTEM

Proposed system aims to bridge this gap by integrating distinguishable features of Keystroke, Mouse and Game play patterns to create a more comprehensive and accurate biometric authentication system. By combining these features, we believe that proposed system will not only improve authentication accuracy but also provide valuable insights into user behavior within games. Proposed system is a new and innovative approach to biometric authentication and game analytics, and we believe that it has the potential to revolutionize these fields. Following Figure 1 depicts the block diagram of proposed system.

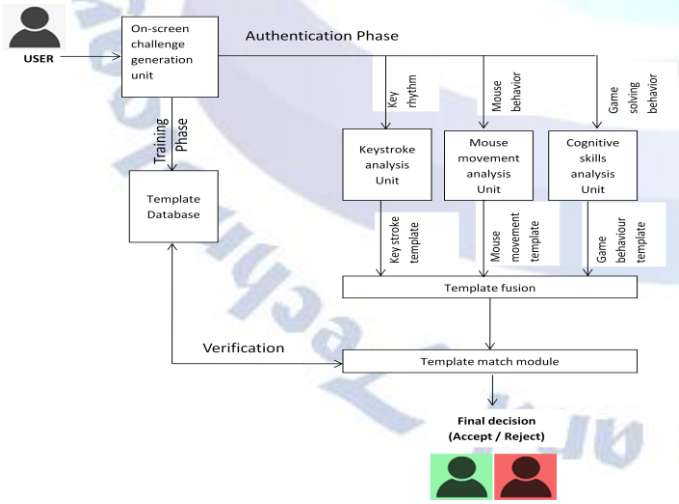


Fig.1. Block diagram of proposed system

The above figure depicts the total outline of the system. The user faces onscreen challenge which includes three steps of authentication. While he is solving the given puzzle, Keystroke, Mouse and Game behaviour analyzers will run in parallel in order to extract the key features and creating a template form such features. Further the user will have a unique template generated by the system saved in the database for future reference. The given template will be matched towards the template save in the database, if it matches, the user is said to be valid else invalid.

Proposed system is designed to provide effective user authentication through the use of cross word puzzle games, while simultaneously tracking keystroke dynamics, mouse dynamics, and game behavior dynamics. By integrating these features, we believe that the system will provide a robust and accurate authentication method that is both secure and user-friendly. The cross word puzzle game will act as an engaging and entertaining platform for users to input their credentials, while the biometric data collected from the user's keystrokes, mouse movements, and game behavior will provide an additional layer of security. By analyzing the unique patterns of these three biometric features, proposed system will be able to accurately authenticate users and prevent unauthorized access. We believe that proposed system will provide a significant improvement over traditional authentication methods and pave the way for new and innovative approaches to biometric authentication.

Proposed system utilizes dynamic cross word puzzles as a means of user authentication, with the unique feature that these puzzles can be generated in an average of 9ms. This quick generation time is crucial for maintaining a seamless user experience, ensuring that users are not left waiting for an extended period to access their accounts. The dynamic nature of the cross word puzzles also adds an extra layer of security, as the puzzles are generated in real-time, making it difficult for malicious actors to replicate or predict the authentication process. With proposed system, users can be confident that their accounts are protected by a secure and efficient authentication method that provides both convenience and peace of mind.

System is designed to provide fast and efficient user authentication, with the added benefit that this process can be completed in just 2ms. This near-instantaneous authentication time ensures that users can quickly and easily access their accounts without any unnecessary delay. The speed of authentication process is made possible by the use of

biometric data collected from keystroke dynamics, mouse dynamics, and game behavior dynamics, which are analyzed in real-time to authenticate the user. By leveraging the power of these biometric features, proposed system is able to provide a high level of accuracy and security while maintaining fast and efficient authentication times. This approach to authentication not only provides users with a seamless experience but also ensures that their accounts are protected against unauthorized access by sophisticated security measures.

Applications of proposed system

The biometric authentication system based on keystroke, mouse, and game behavior has numerous potential applications in various contexts. One possible application is for securing access to computer systems and networks, where it can provide an additional layer of security beyond traditional password-based authentication methods. The system can also be used for online transactions, such as e-commerce and online banking, to ensure secure and reliable user authentication. In the healthcare sector, the system can be used to secure access to electronic health records, ensuring that only authorized personnel can view sensitive patient information. In addition, the system can be applied to the military and government sectors, where high-security authentication is critical for national security. The system can also be used for social media platforms and online gaming, where user authentication is necessary for protecting user privacy and preventing unauthorized access. Overall, the biometric authentication system based on keystroke, mouse, and game behavior has numerous applications in various industries where secure and reliable authentication is critical but not real-time.

5. METHODOLOGY

Proposed biometric authentication system has been developed using Java for the user interface and MySQL for the database. Java is a popular programming language that offers numerous advantages, including platform independence, object-oriented programming, and strong community support. The use of Java for the user interface ensures that the system is both robust and user-friendly, with a wide range of libraries and tools available to enhance the development process. In addition, MySQL is a widely used relational database management system that is known for its reliability, performance, and scalability. By using MySQL for the database, system can efficiently store and retrieve user data, allowing for fast and accurate authentication processes. The combination of Java and MySQL provides a powerful and flexible development environment for the system, ensuring that it is both reliable and easy to use for users.

Totally 16 values are recorded against three biometrics, to create user template. The selected traits are described in the following Table 1.

Table 1. Behaviour and its traits selected

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

The user has to get registered with the application, and he has to solve the puzzle and record his behaviour for at least 15 times, not more than 3 per day. This

restriction is posed to get the best behavioural template of the user which is free from any external restrictions. Normalization of generated templates is essential before generating a unique template, as various factors can affect the values of behavioral biometrics. These factors include physical, environmental, emotional, habitual, and intentional factors, which can cause variations in the biometric data collected from users. Normalization is the process of removing these variations and standardizing the collected data to ensure accurate and consistent analysis. By normalizing the generated templates, proposed system can eliminate the impact of these factors and generate a unique template that is representative of the user's biometric characteristics. This approach enables us to create a reliable and robust biometric authentication system that is not affected by external factors and can accurately identify users with high levels of accuracy. 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 consent of the user to record his Biometrics with the application is recorded during registration. Following Figure.2. is the Registration Page for new User

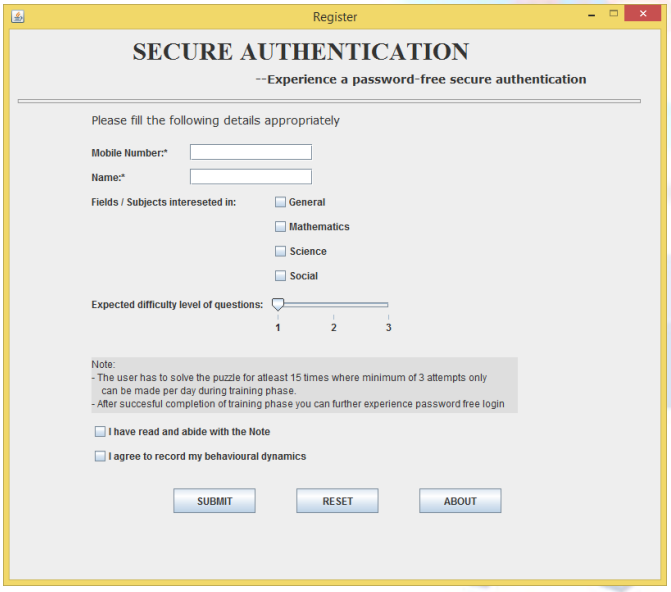


Fig.2. Registration Page

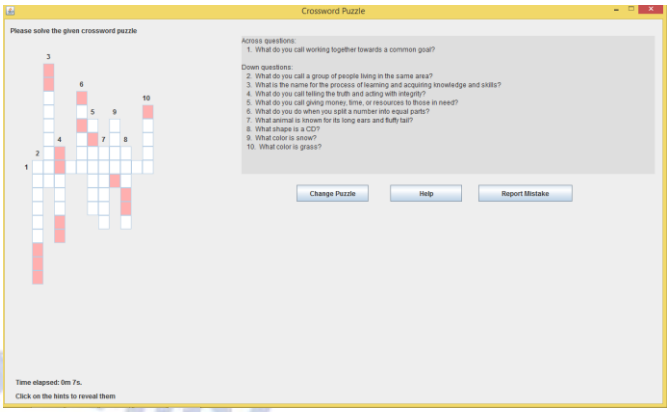


Fig.3. Crossword puzzle

Figure 3 depicts solving the Crossword puzzle. The user has to first click on all hints to reveals them, where Mouse dynamics are recorded. Then the user can start solving the puzzle where Keystroke dynamics are recorded. In the whole procedure, Game dynamics will get recorded. The question database consists of 1000+ handpicked questions. The crossword questions are picked from the database from the respective subjects and level of difficulty which are opted during User registration. Mistakes while solving the puzzle will be marked with Red color and appropriate alphabet will be marked with Green color. Figure 4 depicts solving the crossword puzzle.

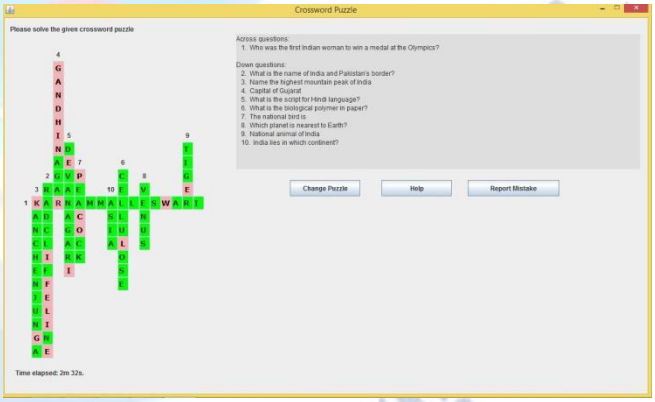
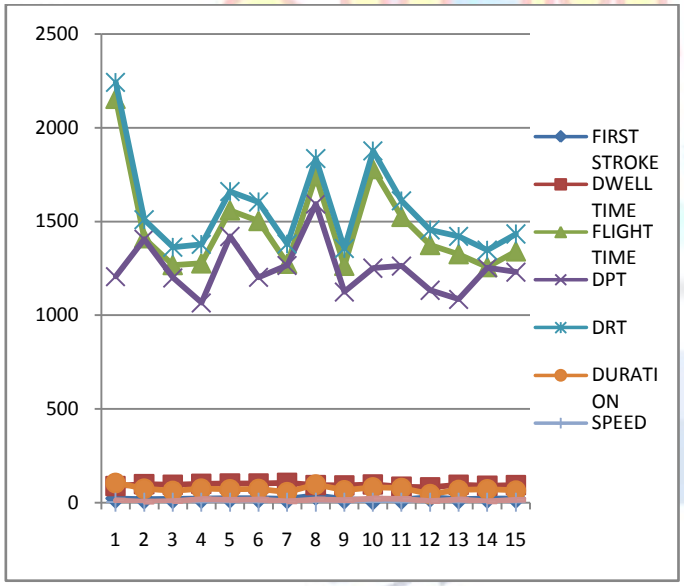


Fig.4. Solving Crossword puzzle

After the training phase completes, the system automatically will generate the template for every user after normalizing the values.

Following infographics Figure 5,6. depicts the user behaviour deviations before and after normalization.

Figure 5. User Game behaviour template before and after normalization



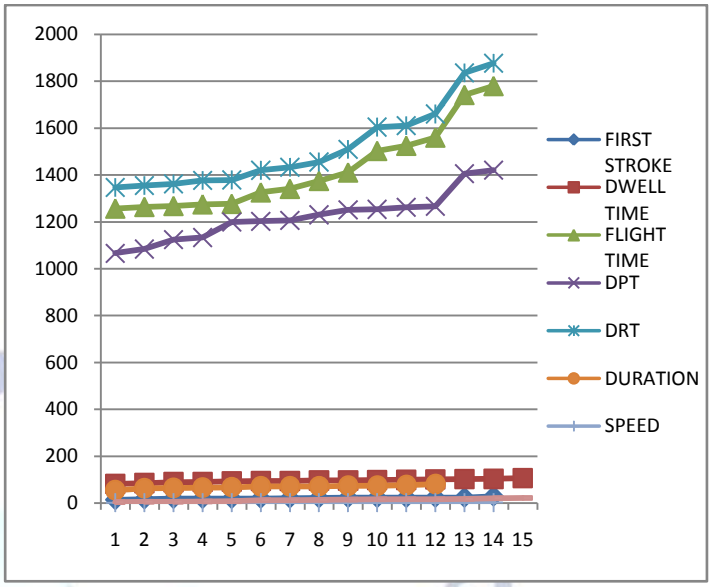


Figure 6. User Key stroke behaviour template before and after normalization

After normalizing the values, Upper boundary and lower boundary of the behaviours are calculated with statistical Inter Quartile range technique. If the reference template lies between the upper and lower boundaries, the user gets authenticated else rejected. Following Figure 7. Depicts the behaviour of the user which falls between upper and lower boundaries and gets authenticated.

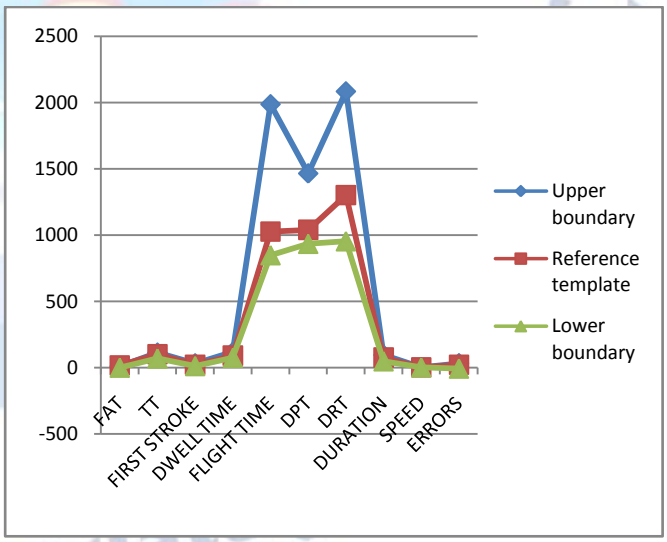


Figure 7. Normal behaviour of the user

Following Figure 8 Depicts the behaviour of the user which falls beyond upper and lower boundaries and gets rejected.

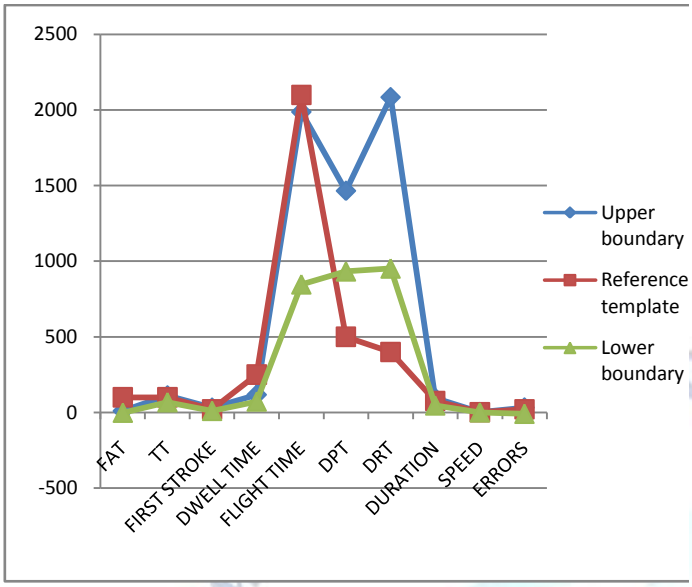


Fig 8. Abnormal behaviour of the user

6. RESULTS

The application is checked with 45 users. 23 users enrolled and verified with the application in our University Computer lab. All the 23 users are Post Graduates. Other 22 users are Graduates and Post Graduates. These users enrolled and verified with the application in their environment. It also checked whether User's behaviour vary from each other even though they all are of same Educational qualification. 10 students of the same class are selected and checked for the same.

The application usability was checked by 100+ users and all the users gave positive feedback for its usability. On a likert scale of 5, 64% of the users gave 5/5, 33.7% gave 4/5, rest of them gave 2/5. This feedback was recorded after the users work with the application for atleast 3 times. The suggestions were also towards positive edge.

According to the evaluation metrics of Biometric systems, the proposed system achieved Failure To Enroll rate - 0%, Failure To Acquire rate - 0%, False Acceptance Rate - 0.6%, False Rejection Rate - 0.04%. The average time taken to generate crossword puzzle User Interface is recorded as 9 ms. The average time taken by the application to accept/reject the user is recorded as 0.03ms. Memory occupied per user is recorded as 111Bytes in My SQL database to save his template.

7. FUTURE SCOPE

The development of proposed biometric authentication system based on keystroke, mouse, and game behavior opens up numerous future research opportunities in the field of behavioral biometrics. One possible avenue for future work is the integration of additional biometric features, such as touch dynamics or facial recognition, to further improve the accuracy and security of the authentication process. Another area for exploration is the use of machine learning algorithms to enhance the performance of proposed system, by enabling it to learn and adapt to user behavior over time. Finally, future research can focus on evaluating the usability and effectiveness of system by conducting extensive user studies, which can provide valuable insights into the user experience and identify areas for further improvement. Overall, proposed biometric authentication system provides a solid foundation for future research and development in the field of behavioral biometrics, with numerous possibilities for innovation and advancement.

8. CONCLUSION

The biometric authentication system based on keystroke, mouse, and game behavior is a promising technology that offers significant benefits in terms of security and usability. By utilizing behavioral biometrics, the system can provide a high level of security that is difficult to replicate or circumvent, making it an ideal solution for high-security and critical systems authentication. Additionally, the use of multiple biometric features increases the complexity of the authentication process, further enhancing the security of the system. The system has a broad scope of applications, with potential uses in various industries, including finance, healthcare, military and government, e-commerce, online gaming, and social media. Overall, the biometric authentication system based on keystroke, mouse, and game behavior represents an exciting development in the field of biometric authentication, with significant potential to improve security and usability in a variety of contexts.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Jain, A.K., Ross, A. and Nandakumar, K., 2016. Introduction to biometrics. Springer.

[2] Ross, A., Jain, A.K., & Nandakumar, K. (2019). Handbook of Multibiometrics (2nd ed.). Springer.

[3] Zhang, D., Zhou, Z., & Chen, S. (2016). Handbook of Biometrics (1st ed.). Springer.

[4] Jain, A.K. (2018). Handbook of Face Recognition (2nd ed.). Springer.

[5] Wang, Y., Li, Y., & Tan, T. (2018). Deep learning for biometrics. Springer.

[6] Bhattacharyya, D., Majumder, S., & Singha Roy, S. (2019). Contactless Biometrics: Concepts, Applications and Limitations. Springer.

[7] Wayman, J. L., Jain, A. K., & Maltoni, D. (2011). Biometric Systems: Technology, Design and Performance Evaluation (1st ed.). Springer.

[8] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). An Introduction to Biometrics. Springer.

[9] Nguyen, D. T., Nguyen, D. H., Nguyen, T. H., & Phan, T. Q. (2021). Continuous User Authentication Based on Keystroke Dynamics Using Recurrent Neural Networks. Sensors, 21(6), 1996. https://doi.org/10.3390/s21061996

[10] Li, Z., Liu, Y., Zhang, Q., Xie, S., & Peng, L. (2020). Keystroke Dynamics as a Secondary Authentication Mechanism for Mobile Devices. IEEE Transactions on Mobile Computing, 19(11), 2527-2539. https://doi.org/10.1109/TMC.2020.2989554

[11] Liu, Y., Li, Z., Xie, S., Peng, L., & Huang, Y. (2019). A Keystroke Dynamics-Based Authentication Method for Smartphones. IEEE Transactions on Mobile Computing, 18(10), 2299-2312. https://doi.org/10.1109/TMC.2018.2863083

[12] Karimian, H., & Faez, K. (2021). A novel mouse dynamics and keystroke dynamics-based biometric authentication system. Computers & Security, 105, 102234. https://doi.org/10.1016/j.cose.2021.102234

[13] Khalid, H., Ahmed, E., Ahmed, E., & Alhajj, R. (2018). Mouse dynamics-based authentication for mobile devices. Computers & Security, 78, 50-64. https://doi.org/10.1016/j.cose.2018.04.001

[14] Faez, K., Karimian, H., & Soltanpour, M. (2018). Mouse dynamics-based continuous authentication using fuzzy adaptive resonance theory neural networks. Journal of Ambient Intelligence and Humanized Computing, 9(6), 1851-1861. https://doi.org/10.1007/s12652-017-0544-2

[15] Gao, X., Wu, Y., Huang, S., & Chen, X. (2020). Analyzing player behavior dynamics in MOBA games: A framework and a case study. Information Sciences, 518, 294-308. https://doi.org/10.1016/j.ins.2019.11.017

[16] Tang, K., Yang, Y., Huang, K., & Lin, Y. (2021). Analyzing player behavior dynamics in MMORPG games: A case study of World of Warcraft. Information Processing & Management, 58(1), 102446. https://doi.org/10.1016/j.ipm.2020.102446

[17] Tseng, C. F., Huang, P. S., & Chiu, C. C. (2018). A game behavior dynamics-based biometric authentication system. Expert Systems with Applications, 113, 353-360. https://doi.org/10.1016/j.eswa.2018.06.035

[18] Sindhu. B and Kezia Rani. B, "Augmenting Biometric Authentication with Artificial Intelligence," IEEE Xplore, *2021 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST)*, Jamshedpur, India, 2022, pp. 340-347, doi: 10.1109/ICRTCST54752.2022.9781908.

[19] Sindhu B, Rani BK. Personnel authentication using multi modal biometrics complemented by cognitive skills. AKNU Journal of Science and Technology 2022; 1(1): 28-35.