User Authentication Using Typing Gesture with Smartwatch

Khandaker Abir Rahman, Kristina Vargo (Mullen), and Avishek Mukherjee

***Abstract*—** A method for enhanced user authentication that relies on sensory data taken from a smartwatch while the user types the username and password has been explored. Eventually, these inherent gestures would work as an added layer of security to the current password-based authentication scheme in a hostile scenario assuming the username-password has been compromised.In our experiments, we recorded the 3D coordinate values given off by the accelerometer and gyroscope over a set of username-password typing combinations. For the sensor data collection, we developed an Android Wear OS smartwatch application, then proceeded to implement our method of sensor data processing and performed experiments to demonstrate the potential of this method. We experimented with 50 samples takenfrom five users, performed 1,800 genuine and impostor authentication attempts, and achieved an equal error rate (EER) as low as 0.07. With such low EER, the proposed method can be aneffective solution to username-password breaches.

***Index Terms*—** accelerometer, biometrics, gesture recognition, gyroscope, sensor data, smartwatch dynamics, user authentication, Wear OS.

I. Introduction and Background

With the most common user authentication, there is typically a username and password combination that a user provides as the credential. This form of authentication, however, neither elicits a sense of security from the user nor is a safe method for authentication because of various attacks due to how the password is crafted, stored, or entered. Therefore, there is a need for a method of user authentication that is more secure against attacks. To make user authentication more secured, several studies proposed various behavioral modalities, including keystroke dynamics (KD) [1,2,3], mouse dynamics [4, 5], touchscreen interaction [6], and device movement [7]. These methods offer new insights into user authentication mechanisms; however, they can come with limitations. Keystroke dynamics have been shown to be less than ideal for user authentication, as shown in [8]. In [8], it was shown that keystroke dynamics are vulnerable to imitation attacks and can prove ineffective at preventing unauthorized users from gaining access to accounts. The work in [9] increased the effectiveness of keystroke dynamics in mobile devices by employing the device's built-in sensors to assist in the authentication of users; however, it is limited to authenticating users only when they are using the device which in turn limits the scope of the system.

To overcome some of the limitations, researchers in recent years have focused on using sensory data given off by smart devices such as smartphones, tablets, or smartwatches as a secondary mode of authentication. These devices, for instance, smartwatches, offer an opportunity to expand the use of the system; however, they introduce their challenges. Although, more recently, the sensors have been considered for user authentication, initial works with smartwatch gesture data involved gesture recognition. For example, the work in [11] explored how effective smartwatch devices were in detecting arm, hand, and finger gestures correctly. It showed viability in detecting unique motions using smartwatch motion sensor data. In similar research, [12] tested fine-motor gesture validity. The work found that the five fine-motor gestures chosen by the authors were recognized with high accuracy. This supports the potential use of gestures for future gesture-based recognition systems. Both works give increased potential viability for using smartwatch motion sensors to detect finite movements, such as the movement of fingers in typing, where the mobility these sensors pick up is limited.

In work more closely related to user authentication, the work in [13] gave users predetermined statements which they were to use to perform a set of tasks, including writing sentences and typing on a keyboard. Results showed high accuracy for user authentication for these tasks. An alternative to predetermined gestures involves gestures that are user-created, or gestures that are chosen by the user. These types of gestures lend themselves more easily to user authentication and validation. The work in [14], [15], and [16] fall into this category. In [14], motion data was collected from individuals who signed their names while wearing a smartwatch. They then used this data to validate and distinguish genuine signatures from falsified signatures. Both [15] and the recent work in [16] offer continuous authentication schemes, both of which are de-signed to correctly identify users while they type, continuously authenticating initial users throughout their sessions. Both offer promising results for the accuracy of identifying users over a longer time versus the short time frame offered from one-time authentication. However, the ability to authenticate users on a one-time login process can be essential for applications in which typing is not the main activity. Securing this process while maintaining ease of use can be challenging. This is where smartwatch motion sensor data for

Manuscript received October 20, 2022. This work was supported in part by the National Aeronautics and Space Administration (NASA) under award number 80NSSC20M0124.

Khandaker Abir Rahman is with the Saginaw Valley State University, Michigan 48603, USA

Kristina Mullen was with the Saginaw Valley State University, Michigan 48603, USA

Avishek Mukherjee is with the Saginaw Valley State University, Michigan 48603, USA

gestures and username-password authentication can work together to provide a robust system for user authentication.

There have been a few works, specifically [17] and [18] where smartwatch typing gestures have been paired with the username-password schema to not only authenticate users but also secure against keystroke inference attacks. These works are closely related to our work; however, [17] is a preliminary study to [18], which contains fewer details and analyses than [18]. In [18], the users were asked to type a predefined QWERTY keyboard password and a predefined keypad PIN into their system while wearing a sensor collecting smartwatch on their right wrist. They then initiated imitation attacks to test the ability of the system to detect genuine users. Both works relied on machine learning classifiers to authenticate users, where they found that their best classifier achieved 4.58% false reject rate (FRR) and 0.12% false acceptance rate (FAR) on the QWERTY keyboard and 6.13% FRR and 0.16% FAR on the numeric keypad. However, the user study conducted in [18] involved only experienced keyboard users, which does not reflect the entire collection of potential users in a real-world setting. Further, the system proposed in [18] does not allow for varying passwords in different websites which again, does not reflect well in a real-world scenario where users are encouraged to have varying passwords for different accounts.

Our method seeks to authenticate users using alternative methods. For authentication, the smartwatch typing gesture that we explore in this paper is paired with a username-password system for user authentication. The method we developed is intended to authenticate a user in a connected device (by logging into a computer, un-locking a smartphone screen, etc.) via Bluetooth or Wi-Fi connectivity. Our experiment involved five users and 50 samples collected by our developed smartwatch app. We then implemented our own method to process data and showed the efficacy of a range of experiments. The paper is organized as follows. We discuss the data collection process in Section II. Section III describes the data processing methods and characteristics of the data. Section IV demonstrates the error computation method. Experimental setups, results are presented in Section V, and we conclude in Section VI.

II. Data Collection

Using an Android platform, we developed a simple application that can be used on smartwatches that use the Android Wear OS operating system. This app is compatible with devices running SDK 30 (Android 8.0) or higher and consists of a simple user interface that displays a single button that is used to start-stop the recording accelerometer and gyroscope data. Internally, the Android's Sensor Manager class was used to gain access to the raw accelerometer and gyroscope sensor data and subsequently log those values as they were taken in. The capture of this raw data was taken as quickly as the hardware allowed access to both the sensors. For both accelerometer and gyroscope, this was around the rate of 5Hz. Finally, the data for each experiment were locally stored in the smartwatch as a comma-separated text file and transferred to a common Wi-Fi connected Windows 10 workstation using the Android Debug Bridge (ADB) tool.

The device used for data collection was a Fossil Gen 4 Carlyle smartwatch that ran on the Wear OS and was paired to an Android smartphone. For the experiment, five volunteers were selected as users. The collection was done on the same day in two parts. In Session I, each user was asked to come up with two phrases, one to use as their own fictitious username and the other to use as a fictitious password.

Information regarding the selection of these username-password combinations:

- Each combination was separated by a single press of the Enter key.
- No limitations were placed on what these phrases should consist of other than to ensure the user used no direct references to themselves or their associated current accounts.
- Over the selected usernames, the number of characters in the username ranged from nine to fourteen. These characters were made up of letters a-z and numbers 0-9. Not every username contained both letters and numbers, as the decision was left up to user preference.
- Over the selected passwords, the number of characters in the password ranged from ten to fourteen. These characters were made up of letters a-z, numbers 0-9, and symbols. Not every password contained all these elements, but instead, there was a variance among the passwords based on user choice if they included them or not.

The user was then given time to practice the combination until they felt comfortable with the movements. Once comfortable, the user was given a smartwatch, with our developed application already loaded and paired to the researcher's Android phone and Windows 10 device, which the user was then asked to secure to their dominant hand. When the watch was secured, each user was then asked to press the start-stop button on the application, wait for a calibration periodof around six seconds, proceed to type their passphrase combination, and then pause for a resting period of around six seconds once the typing was complete. This was repeated a total of five times for each user. If a mistake was made while the user was typing, the data collection process was restarted from the beginning. A total of twenty-five samples were taken during Session I.

Part II consisted of the same structure as Part I, with the only change being instead of the user creating two phrases of their own, two passphrases were given to each user by the researcher. These two passphrases for username and password, "UserName” and “P4sswOrd” respectively, were the same for every user. Each user repeated this a total of five times, which resulted in a total of twenty-five samples taken in Session II.

III. Data Processing

As mentioned above, each experiment was prefaced with a stationary resting period to synchronize the sensor data across experiments. Thus, before any comparison can be made, each of these measurements needs to be aligned properly. The alignment was done using a heuristic-based method that works well for the collected data. Initially, a base threshold is established by looking at a window of sensor values from the

stationary period. The base threshold was measured using the mean and standard deviation of the measurements. Specifically, the threshold is computed as the mean value added with four times the standard deviation. This was done on 10 samples from the middle of the stationary period. The idea is that when the actual movement starts, the statistics from a moving window of the same size should comfortably exceed the base threshold measured above. This was repeated for both the accelerometer and gyroscope data across all three axes. A similar process was followed to compute the ending point of the movement.

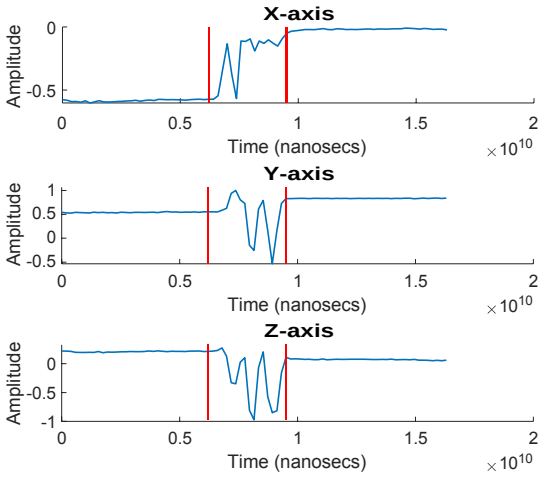

Fig. 1. The outcome of the alignment method to identify the start and end of the movement

An example of the alignment result can be seen in Fig 1, where the amplitude of the signal measured on all three axes on the accelerometer is shown. The vertical barriers indicate the subset of the signal data that is clipped and considered during the preprocessing stage. It can be seen that the alignment method described above works very well to identify the start and end times of the movement.

IV. Error Computation Method

The difference between the reference and authentication/test measurements is computed by first aligning the measurements using the process described in Section 3. Next, the longer of the two measurements is truncated such that both measurements have the same number of samples. The error is computed by averaging the pointwise squared error between each pair of measurements. This process is repeated on all axes and for both the gyroscope and accelerometer data.

As an example, figures 2, 3, and 4 show the computational error when using the accelerometer data across two sets of measurements. Fig 2 shows the aligned signals on each of the three axes when comparing a pair of signals that belong to the same user typing the same password. Naturally, after correct alignment, the signal data shows similarity. On the other hand, Fig 3 shows the aligned signals when looking at signal data from two different users typing different passwords. Visual dissimilarity is evident in this case.

After looking into the obvious similarity in aligned data for the same user typing the same password and dissimilarity for different users typing different passwords, the question remains how it looks for different users typing the same password. Assuming the username-password has been compromised, would the typing gesture be enough to differentiate between the impostor and genuine users? To answer the question, we emphasized comparing sensor data when the same username-password was typed by different users. The experimental results show interesting findings indicating significant dissimilarity when the same username-password wastyped by different users in a hos-tile scenario. In Fig 4, a level of dissimilarity is shown for two users (user 3 and user 4) typing the same username-password.

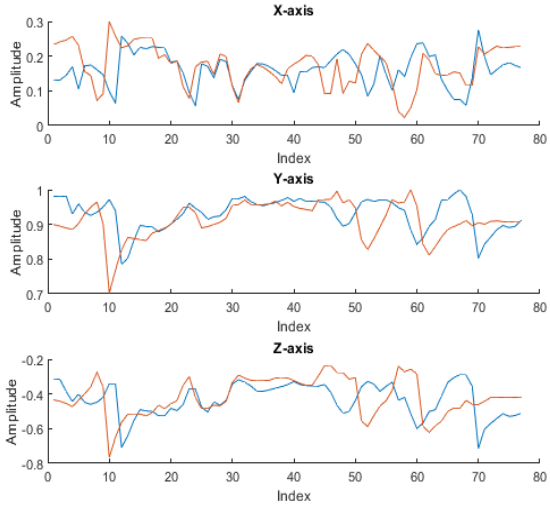

Fig. 2. Accelerometer sensor data on three axes for two different samples of the same user while typing the same username-pass-word.

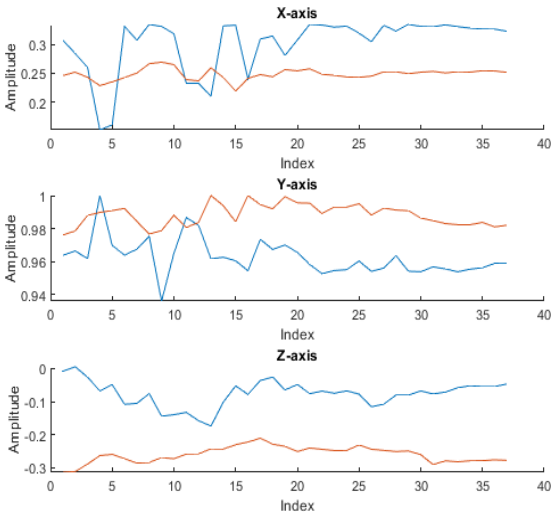

Fig. 3. Accelerometer sensor data on three axes for two samples of the two different users while typing different username-pass-words.

The numerical measures to find similarity (or dissimilarity) between samples are done by computing the sum of the squared error between corresponding timestamps across any two samples across all axes and sensors. Fig 5 below shows a comparison between the combined average error on all axes when comparing signals belonging to the same user typing the same username-password. As shown, the overall error measured re-mains below 0.02 for 80% of the data points. On the other hand, inter-pattern (i.e., different users typing the same username-password) comparisons successfully resulted in a higher combined error across all sensors.

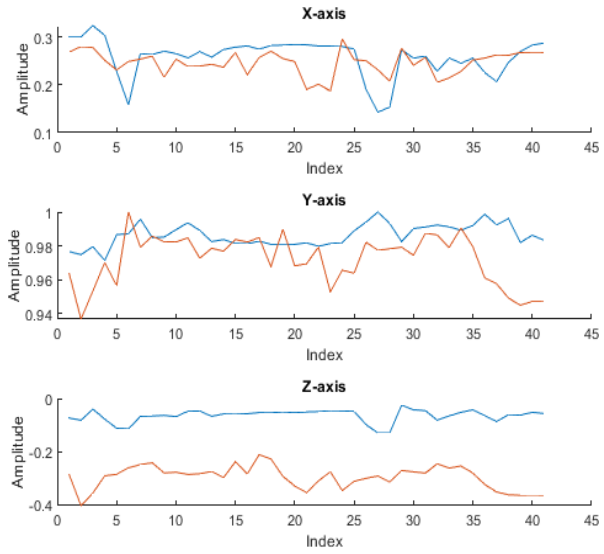

Fig. 4. Accelerometer sensor data on three axes for two samples of the two different users while typing the same username-password.

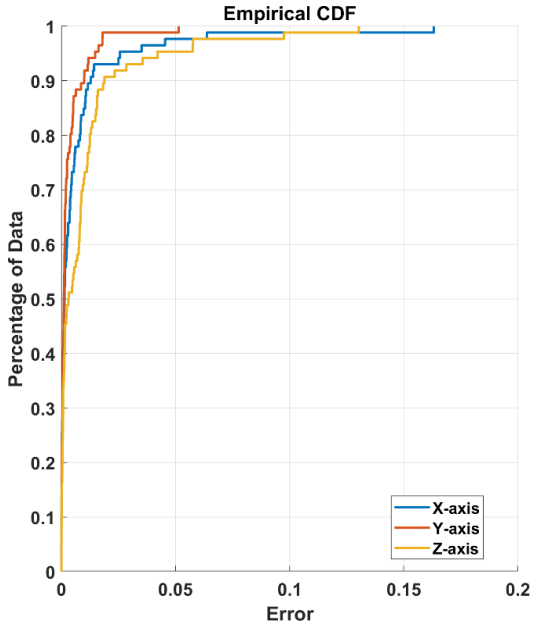

Fig. 5. Error plots on three axes when comparing two samples of the same user while typing same username-password.

V. Experimental Setups and Results

To measure the performance of our method, we performed a series of genuine and impostor attempts and calculated Impostor Pass Rates (IPR) and False Rejection Rates (FRR). For genuine attempts, all five users' five samples collected during Session I are compared with each other. For instance, the sample $S_{i,j}$ is compared with the sample $S_{i,k}$ where i is the user number and j, k are sample numbers for that user. For genuine attempt comparisons, $i, j, k = 1$ to 5 and $j \neq k$. A total of 50 combinatorial comparisons are considered for each axis over a sensor. Considering the three axes and two sensors, there are 300 genuine authentication attempts.

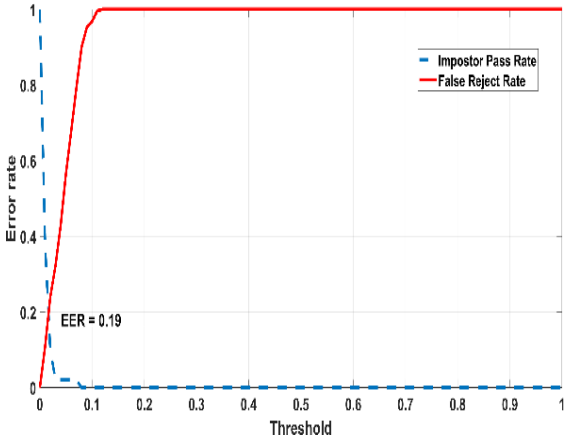

Fig. 6. Impostor pass rate and false rejection rate for X-axis data of accelerometer. The EER found is 0.19.

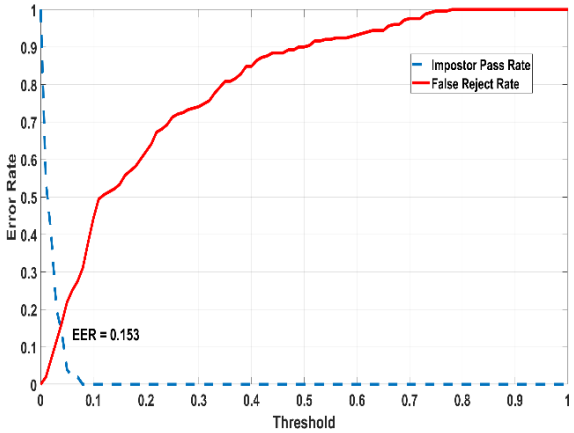

Fig. 7. Impostor pass rate and false rejection rate for Z-axis data of accelerometer. The EER found is 0.153.

The IPR Vs. FRR plots are shown in figures 6 to 9, respectively for accelerometer X-axis (Fig 6), Z-axis (Fig 7), X and Z axes combined (Fig 8), and for gyroscope X, Y, Z axes combined (Fig 9). The EER values are shown near the crossover points.

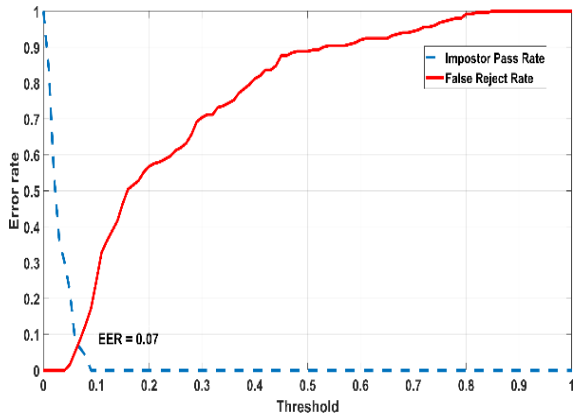

Fig. 8. Impostor pass rate and false rejection rate for X and Z axes combined data of accelerometer. The EER found is 0.07.

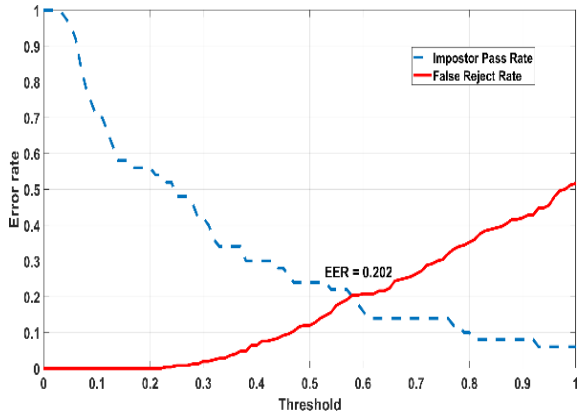

Fig. 9. Impostor pass rate and false rejection rate for X, Y, and Z axes combined data of gyroscope. The EER found is 0.202.

TABLE I: Average Error Rates for Accelerometer Data

Sample Comparison	Average Error Rate			
	X-axis	*Y-axis*	*Z-axis*	*X + Z*
Genuine Scores				
User 1 Vs User 1	0.01595	0.03405	0.04126	0.05721
User 2 Vs User 2	0.00449	0.46293	0.01409	0.01859
User 3 Vs User 3	0.0204	0.35874	0.01042	0.03082
User 4 Vs User 4	0.00459	0.21821	0.02077	0.02536
User 5 Vs User 5	0.00696	0.17744	0.00602	0.01298
Impostor Scores				
User 1 Vs User 2	0.04712	0.71592	0.32188	0.369
User 1 Vs User 3	0.03076	0.63223	0.37472	0.40548
User 1 Vs User 4	0.02352	0.19179	0.14817	0.17168
User 1 Vs User 5	0.06316	0.64109	0.63737	0.70053
User 2 Vs User 3	0.05657	0.88493	0.02335	0.07992
User 2 Vs User 4	0.05056	0.75938	0.04759	0.09815
User 2 Vs User 5	0.01042	0.37612	0.10719	0.11761
User 3 Vs User 4	0.01362	0.65797	0.08581	0.09943
User 3 Vs User 5	0.08421	0.30648	0.05532	0.13953
User 4 Vs User 5	0.0708	0.67779	0.21817	0.28897

TABLE II: Average Error Rates for Gyroscope Data

Sample Comparison	Average Error Rate			
	X-axis	*Y-axis*	*Z-axis*	*Total*
Genuine Scores				
User 1 Vs User 1	0.31447	0.02824	0.09616	0.43887
User 2 Vs User 2	0.52375	0.25332	0.53718	1.31425
User 3 Vs User 3	0.15095	0.01606	0.41953	0.58654
User 4 Vs User 4	0.61538	0.04863	0.08742	0.75143
User 5 Vs User 5	0.45749	0.38397	0.53083	1.37229
Impostor Scores				
User 1 Vs User 2	0.4399	0.14979	0.58171	1.17141
User 1 Vs User 3	0.303	0.02991	0.30878	0.64169
User 1 Vs User 4	0.36437	0.04227	0.10796	0.5146
User 1 Vs User 5	0.48527	0.26128	0.38453	1.13108
User 2 Vs User 3	0.28139	0.17054	0.52052	0.97245
User 2 Vs User 4	0.50071	0.204	0.57041	1.27542
User 2 Vs User 5	0.44722	0.34107	0.74088	1.52916
User 3 Vs User 4	0.37465	0.02602	0.23418	0.63486
User 3 Vs User 5	0.3905	0.23708	0.45256	1.08014
User 4 Vs User 5	0.68975	0.23423	0.42053	1.34451

For impostor attempts, all possible inter-user sample combinations are considered over Session II data, where all the users typed the same username and password. For instance, the sample $S_{i,j}$ is compared with the sample $S_{m,n}$ where i, m are users and j, n are sample numbers for that user. For inter-user impostor comparison, $i, j, m, n = 1$ to 5 and $i \neq m$. A total of 250 combinatorial inter-user impostor comparisons are considered for each axis over a sensor. Considering the three axes and two sensors, there are 1,500 impostor authentication comparisons. Therefore, a total of 1,800 authentication attempts (genuine and impostor combined) are considered for the experimental results.

For each genuine or impostor attempt, the error rate for 80% of data points (as shown in Fig 5) was noted. Therefore, a total of 1,800 error rates were generated. To summarize, the average error rates were taken when comparing multiple samples within the same user (for genuine attempts) or between two different users (for impostor attempts). The summarized accelerometer and gyroscope error rates are shown in tables 1 and 2, respectively.

The findings from the tables can be summarized as follows:

- The genuine scores are significantly lower than impostor scores, especially for accelerometer data.
- It is also noticeable that the accelerometer, in general, performs better by giving off lower error rates compared to the gyroscope errors for genuine attempts. This out-lines a higher level of differentiability between genuine and impostor attempts.
- Among accelerometer axes, X and Z axes perform better compared to Y axis by giving off high differentiability between genuine and impostor attempts, i.e., lower genuine scores and higher impostor scores.
- Inspired by the better performances of the accelerometer's X and Z axes, the total of X-Zscores were calculated (see the last column in Table 1) to achieve better overall differentiability. For thegyroscope, the total for all three axes was considered (see the last column in Table 2).

To measure the detection-error performance of the system, we calculated the IPR and FRR over the threshold values from 0 to 1. Note that the error value 0 indicates a perfect match and 1 for a complete mismatch. The threshold step size was selected as 0.001; therefore, a total of 1,000 IPR and FRR values were calculated over the thresholds. After plotting the 1,000 IPR and FRR values, the equal error rate, EER (i.e., the cross-over point, where the IPR and FRR values are equal), has been calculated.

The EER values for other experimental setups, for instance, accelerometer Y axis, gyroscope X axis, were all calculated but not shown here. In general, the EER values for accelerometer data are found lower (as shown in Fig 6, 7, and 8, for instance) compared to gyroscope data (as shown in Fig 9). Among all the setups, the lowest EER value of 0.07 was found for accelerometer X, and Z axes combined data as shown in Fig 8. In other words, the authentication error remains only 7% for accelerometer data when X and Z axes are combined. With such impressive low EER, our method shows its potential to be a standalone biometric modality for user authentication.

VI. Conclusion and Future Works

This research work demonstrates a novel method for user authentication based on typing gestures. We collected sensor data using our developed Android Wear OS smartwatch app. A total of 50 samples were used to perform 1,800 genuine and impostor authentication attempts. With this, the impostor pass rates, and false reject rates were generated, varying 1,000 thresholds for each experimental setup. From there, our method achieved an equal error rate (EER) as low as 7%. We believe the scope for decreasing the EER of our method is still wide and deep. Therefore, for future works on this topic, we can consider the following for immediate improvements of our methodology – (1) preprocessing our data to remove/observe outliers, and (2) fusion of accelerometer and gyroscope data to get combined authentication decision. We argue that this typing gesture could be a strong standalone biometric modality as well as a secondary security measure when the username-password based authentication has been compromised.

Acknowledgment

Research reported in this publication was supported in part by funding provided by the National Aeronautics and Space Administration (NASA) under award number 80NSSC20M0124.

References

[1] D. Gunetti, C. Picardi, "Keystroke analysis of free text," ACM Trans. Information, System, Security, vol. 8, no. 3, pp. 312–347 (2005). https://doi.org/10.1145/1085126.1085129

[2] K. A. Rahman, D. Neupane, A. Zaiter, and M. S. Hossain, "Web User Authentication Using Chosen Word Keystroke Dynamics", Int Conf on Machine Learning & Applications, (2019). https://doi.org/10.1109/ICMLA.2019.00188

[3] F. Monrose, A. Rubin, "Authentication via keystroke dynamics", Proc. of the 4th ACM Conference on Computer and Communication Security, pp. 48–56, NY, USA (1997). https://doi.org/10.1145/266420.266434

[4] K. A. Rahman, R. Moormann, D. Dierich, and M. S. Hossain, "Continuous User Verification via Mouse Activities", Int Conf on Multimedia Communications, Services and Sec, (2015). https://doi.org/10.1007/978-3-319-26404-2_14

[5] C. Shen, Z. Cai, X. Guan, Y. Du, R. Maxion, "User Authentication Through Mouse Dynamics", IEEE Trans. Inform. Forensic Security., vol. 8, no. 1, pp. 16-30 (2013). https://doi.org/10.1109/TIFS.2012.2223677

[6] K. A. Rahman, J. Maes, "How Discernible User Impromptu Behavior is When Unlocking Touch Screen?", Int Conf on Computer and Information Technology, Bangladesh (2017). https://doi.org/10.1109/ICCITECHN.2017.8281788

[7] K. A. Rahman, D. J. Tubbs, M. S. Hossain, "Movement Pattern Based Authentication for Smart Mobile Devices," 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Florida, USA, pp. 1054-1058 (2018). https://doi.org/10.1109/ICMLA.2018.00172

[8] C. Meng, G. Payas, and G. Debin. "I Can Be You: Questioning the Use of Keystroke Dynamics as Biometrics", Annual Network and Distributed System Security Symposium. Re-search Collection School Of Computing and Information Systems (2013).

[9] C. Giuffrida, K. Majdanik, M. Conti, H. Bos, "I Sensed It Was You: Authenticating Mobile Users with Sensor-Enhanced Keystroke Dynamics", In: Dietrich S. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2014. Lecture Notes in Computer Science, vol 8550. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-08509-8_6

[10] X. Liu, Z. Zhou, W. Diao, Z. Li, and K. Zhang, "When Good Becomes Evil: Keystroke Inference with Smartwatch", In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15). NY, USA, 1273–1285 (2015). https://doi.org/10.1145/2810103.2813668

[11] C. Xu, P. H. Pathak, P. Mohapatra, "Finger-writing with smartwatch: A case for finger and hand gesture recognition using smartwatch", Proceedings of the 16th International Work-shop on Mobile Computing Systems and Applications (HotMobile '15). Association for Computing Machinery, New York, NY, USA, 9-14 (2015).

[12] H. Wen, J. R. Rojas, A. K. Dey, "Serendipity: Finger gesture recognition using an off-the-shelf smartwatch", Proceedings of the 2016 CHI Conference on Human Factors in Compu-ting Systems (CHI '16). Association for Computing Machinery, 3847-3851 (2016). https://doi.org/10.1145/2699343.2699350

[13] F. Ciuffo, G. M. Weiss, "Smartwatch-based transcription biometrics," Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, pp. 145-149 (2017). https://doi.org/10.1109/UEMCON.2017.8249014

[14] G. Li, H. Sato, "Handwritten Signature Authentication Using Smartwatch Motion Sensors," Annual Computers, Software, and Applications Conference, Spain pp. 1589-1596 (2020). https://doi.org/10.1109/COMPSAC48688.2020.00-28

[15] B. Li, H. Sun, Y. Gao, V. V. Phoha, Z. Jin, "Enhanced free-text keystroke continuous authentication based on dynamics of wrist motion," Workshop on Information Forensics and Security, pp. 1-6 (2017). https://doi.org/10.1109/WIFS.2017.8267642

[16] A. Acar, H. Aksu, A. S. Uluagac and K. Akkaya, "A Usable and Robust Continuous Authentication Framework Using Wearables," IEEE Trans on Mobile Computing, vol. 20, no. 6, pp. 2140-2153 (2021) https://doi.org/10.1109/TMC.2020.2974941

[17] B. Chang, X. Liu, Y. Li, P. Wang, WT. Zhu, “Employing smartwatch for enhanced password authentication”, L. Ma, A. Khreishah, Y. Zhang, M. Yan (eds), Wireless Algorithms, Systems, and Applications, Lecture Notes in Computer Science, vol 10251. Springer (2017). https://doi.org/10.1007/978-3-319-60033-8_59

[18] B. Chang, Y. Li, Q. Wang, WT. Zhu, R. Deng, “Making a good thing better: enhancing password/PIN-based user authentication with smartwatch”. Cybersecurity 1, 7 (2018). https://doi.org/10.1186/s42400-018-0009-4

Khandaker Abir Rahman is a Professor of Computer Science at Saginaw Valley State University, Michigan, USA. He received his Ph.D., MS in CS, MS in Mathematics from the Louisiana Tech University, and his BS, MS in CSE from the University of Dhaka, Bangladesh. His research interest includes behavioral biometrics, cybersecurity, machine learning and artificial intelligence. He co-authored 25 research articles in refereed journals, international conferences, and five book chapters. He has been working as reviewer for several high impact journals. He is the SVSU’s representative for Michigan Space Grant Consortium (MSGC). In 2021, he was awarded the senior member status of Association of Computing Machinery (ACM) and Institute of Electrical and Electronics Engineers (IEEE).

Kristina Vargo (Mullen) received her B.S. from Saginaw Valley State University. She was awarded the Michigan Space Grant Consortium's undergraduate research fellowship for the 2021-2022 school year for proposed research work in the field of Cybersecurity.

Avishek Mukherjee is an Associate Professor of Computer Science at Saginaw Valley State University, Michigan, USA. He received his Ph.D. and MS in Computer Science from Florida State University. His research interests include wireless networks and systems with an emphasis on physical layer algorithms. He has been awarded several internal research grants at Saginaw Valley State University as well as a research seed grant from the Michigan Space Grant Consortium in 2020. In addition to his research, he also serves as the faculty advisor for the Association of Computing Machinery chapter at SVSU.