A New Approach for Textual Password Hardening Using Keystroke Latency Times

Khalid Mansour[1] and Khaled Mahmoud[2]
[1]Faculty of Information Technology, Zarqa University, Jordan
[2]King Hussein School of Computing Sciences, Princess Sumaya University for Technology, Jordan

Abstract: *Textual passwords are still widely used as an authentication mechanism. This paper addresses the problem of textual password hardening and proposes a mechanism to make textual passwords harder to be used by unauthorized persons. The mechanism introduces time gaps between keystrokes (latency times) that would add a second protection line to the password. Latency times are converted into discrete representation (symbols) where the sequence of these symbols is added to the password. For accessing system, an authorized person needs to type his/her password with a certain rhythm. This rhythm is recorded at the sign-up time.This work is an extension to a previous work that elaborates more on the local approach of discretizing time gaps between every two consecutive keystrokes. In addition, more experimental settings and results are provided and analyzed. The local approach considers the keying pattern of each user to discretize latency times. The average, median and min-max are tested thoroughly.Two experimental settings are considered here: laboratory and real-world. The lab setting includes students studying information technology while the other group are not. On the other hand, information technology professional individuals participated in the real-world experiment. The results recommend using the local threshold approach over the global one. In addition, the average method performs better than the other methods. Finally, the experimental results of the real-world setting support using the proposed password hardening mechanism*.

Keywords: *Textual password, password hardening, latency time, keying pattern, discretization*.

Received April 26, 2020; accepted November 18, 2020
https://doi.org/10.34028/iajit/18/3/10

1. Introduction

Electronic devices are widely used and most of them have an authentication process to grant access to either the device itself or to the applications installed on it. The wide spread of electronic devices and computer systems is associated with an increased concern in information security. The authentication issue is one of the top ten recognized security risks in the web [44]. Moreover, as shown by the US Federal Trade Commission, identity thefts affects millions of consumers every year [14]. Therefore, authentication methods and password hardening are important research areas that attract the attention of the research community [9, 12, 28, 31, 39, 42, 48].

Different types of authentication methods are studied and employed [13, 22, 36]. However, Textual passwords are stillthe most used and practical authentication method [16]. Forthe rest of this manuscript, password and textual passwordare used interchangeably. Passwords can be either standaloneor be part of other authentication mechanisms [2, 10, 19].

As mentioned in [15] "despite long known shortcomings inboth security and usability, passwords are highly unlikelyto disappear". One of the important advantages of textualpasswords is that they do not need extra equipment or violateprivacy. In addition, textual passwords can be more immune to shoulder-surfing attacks than graphical authentication methods that depend on picture-recognition [26]. Regarding the disadvantages of textual passwords, users may choose passwords that can be easily guessed or cracked [25].

This work extends our previous work [31] by:

1. Introducing new discretizing methods.
2. Collecting experimental results from a larger group of participants.
3. Introducing a real-life experiment.

The work in [31] proposed authentication mechanismsfor creating passwords that considers the ability ofusers to adopt certain password keying patterns when creatingtheir passwords. Users need to use the same keying rhythmswhen they wish to sign-up into their accounts. The keyingrhythm involves introducing relatively large or small time gaps (latency times) when typing their password characters at thesign-up time. The latency times are converted into symbolsusing certain thresholds. These symbols become part of thetextual password which hardens it and eventually improvethe authentication system. This method is effective to protectsystems in case the passwords are stolen or the users chooseeasy to guess passwords since it is difficult for impostor usersto guess the rhythms of passwords.

The password keying pattern is registered as a sequence of F(fast)/S(slow) symbols. A latency time is labeled as either For S using a certain threshold value. The threshold value canbe either global or local. The

global threshold value dependson the collective keying patterns of a group of users whilethe local threshold value depends on the individual keyingpatterns of individual users. Since the work presented in [31] recommends using local threshold values in the process ofgenerating the symbols F or S, this paper considers the localthresholds values only. For the local threshold values: average, median and min-max mechanisms are investigated in discretizinglatency times into either F or S. A number of measuresare used to evaluate different discretizing mechanisms suchas true positive rate and false positive rate. More details arepresented in the following sections.

As Keystroke Dynamics (KD) refers to the quantitative dataobtained from the keying activities of users such as the overallspeed and variations of speed movements between certain keys [24], this research uses the elapsed time between keying twoconsecutive characters of a textual password to harden textualpasswords. This keystroke feature is adopted by users andcollected only at the sign-up time. Other related studies basedon keystroke dynamics collect keystroke dynamics data fromusers over a certain period of time then the collected data needto analyzed using machine learning or statistical methods forpossible detection of genuine users or password hardening [18, 34, 45, 47].

The password hardening mechanism proposed in this paperis not concerned about analyzing the behaviors of users whenkeying their characters over a certain period of time, it ratherasks each user to adopt a unique keying rhythm which willbe part of his/her password. The main disadvantage of other related keystroke dynamics-based methods is that they requiretime for collecting the keying behaviors of users before thesystem can be deployed [45]. In addition, adaptive algorithms [11] need to use in case of users change their typing stylesafter some time, e.g., they become faster in typing, otherwise,a new data need to be collected and analyzed before the systembecomes effective again. Moreover, in some KD algorithms, anumber of factors can negatively affect the verification processsuch as stress and emotions [46].

Finally, in many cases, users may choose passwords that areshort and easy to remember. Moreover, some authenticationsystems require users to follow a number of rules in choosingtheir passwords such as requiring a minimum number ofcharacters for the password. However, some users may not follow these policies [35]. This behavior of users can be ofa less harm when using the proposed password hardeningmechanism since it can effectively protect short and easy toguess passwords.

The main contributions in this paper are summarized asfollows:

- Investigating new local threshold methods for discretizing latency times.
- Presenting and analyzing new experimental results. for a larger sample of participants.
- Resenting results of a real-life experiment.

The rest of this paper is organized as follows: section 2 reviews the related work. Section 3 presents the adoptedkeystroke rhythm mechanism. Section 4 introduces the experimentalmethodology and the results are discussed in section 5. The practicality of the proposed password hardening mechanismis discussed in section 6. Finally, section 7 presents the conclusion future work.

2. Related Work

Authentication systems are integral part of anyinformationsystem. Therefore, important theoretical and application workis dedicated to improving the performance of authentication processes, such as [1, 47].

Authentication mechanisms can be categorized as: knowledge-based (what you know), token-based (what youhave) and biometric (what you are). Differentauthenticationmechanisms are suggested under each category, e.g., [4]. Textual passwords are examples of the first type. The graphical password in another example [10, 38].

A combination of two or more mechanisms is also used asauthentication mechanisms. For instance, different bank systemscombine both knowledge-based and token-based authentication mechanisms [37]. Some other systems use biometricauthentication mechanisms which classify individuals basedon their physical traits (e.g., Iris recognition) or behavioral characteristics [20, 33]. For example, typing dynamics is consideredas an important biometric behavior feature [3] because previous studies claim the hypothesis that different individualscan be classified based on their typing styles [38].

Keystroke dynamics has been there for a while, its use foridentification purposes started in the 1970s [43]. Keystrokefeatures are used to either harden passwords or characterizeindividuals by their typing pattern [27] [34]. Research onkeystroke dynamics is based on either fixed-text or free-textinput data. A number of studies consider using the fixed-textdata where the keystroke dynamics focuses on analyzing thedynamics of keying a fixed input -mostly a password-for authenticating users [47]. Free-text input analyzes the wayusers interact with the keyboard during a session, the studypresented in [21] shows that non-English words served betterthan English words in identification.

Several machine learning techniques to identify and classifyusers are employed to improve the results of keystroke dynamictechniques. For example, K-Nearest Neighbor (KNN) classifiers [6], Fuzzy logic [17] and Support Vector Machines (SVMs) [41] are used to

improve the authentication outcomes. For comprehensive surveys see [46, 47]. The disadvantageof keystroke dynamic-based authentication mechanismsis that an intensive learning is required before the system canbe ready for use. In addition, users may change their typingstyles over time, therefore the authentication systems need toperform the learning phase again [32, 34]. Moreover, changesdue to temporal factors such as stress and various emotionstates may affect the results of the learning phase [46]. Inaddition to keystroke dynamics, keystroke sound is also usedto authenticate users [40].

The interaction with the 3-D environment is another authenticationscheme. In such a scheme, a user needs to interactwith a 3-D environment. The user is required to perform acertain predefined sequence of actions to be authenticated bya system. For example, the user may choose his password tobe the following sequence of actions: finger print, start a carand finally use an ATM machine. The disadvantage of thiskind of authentication system is its requirement for a set ofequipment such as finger print reader which increases the costof using such systems [2].

The work presented in [29, 31, 34] is amongst the mostrelated works to this paper. The study presented in [34] considers the latency times and duration times for passwordhardening. It combines the keystroke dynamics results withthe textual password. This method needs a training time beforeit can be used. This method has a positive feature because itadjusts the password-hardening data after each successful sign-in.However, if the typing style of users change significantlyfrom the styles of previous successful sign-ins, the sign-inprogram becomes not successful in generating the requiredpassword-hardening data.

The password hardening mechanism shown in [29] concatenatesthe types of time gaps (e.g., fast/slow) between passwordcharacters to the textual password. However, the difference isthat the users in [29] are given the option to determine thetypes of time gaps between password characters at the sigh-upof time gaps between password characters, the research in [30] showed how a password file theft can be detected usingthe extra information about how fast/slow users type theirpasswords.

The work presented in [5] is similar to our work except thatit requires a user to register his/her personalized private styleusing mouse clicks. The first part of the experiment, the systemcollects the rhythm features of the mouse clicks. The collectedfeature samples are used to train a classifier. The system usesthe clicked target rhythm to verify a user by examining anumber of features which are: down-up, down-down and up-down. Our paper depends on the style of typing the passwordrather than using mouse clicks and at the sometime, ourmethod does not require a classifier therefore no learningphase is required. The fixed-text input is considered in this paper whichmakesour work unique is that the proposed system does not require alearning step before the system starts operating and it does notanalyze the keystrokes of users. The proposed authenticationsystem asks users to adopt certain keying styles when choosingtheir passwords during the sign-up phase. The keying rhythmsof users become part of their passwords. In addition, severalmechanisms are proposed and tested to discretize latencytimes. Finally, results for real time experiments are presentedand analyzed.

The results shown in this paper are equal or better thanthe results presented in [31]. The reason is that the number ofparticipants used in this paper is larger than the one used in [31]. Moreover, this paper presents a life-experiment resultswhich consolidate the effectiveness of the proposed passwordhardening method.

3. Adopted Keystroke Rhythm Mechanism

Keystroke rhythm is the style of typing characters on a keyboard. The time gaps-measured in milliseconds (ms) between every two consecutive characters is the latency times which are captured and processed as illustrated in this section. When key k2 is pressed after key k1 then the latency time $(lt_2)=T(k_2)-T(k_1)$, where T is a function that is used to get the current computer time at K_i. For a set of n consecutive keystrokes for a user, i, $Lt_i = <lt_2^i, lt_3^i,..., lt_n^i>$ see Algorithm 1. The sets $LT_g = \{Lt_1^g, Lt_2^g, Lt_3^g,..., Lt_m^g\}$ and $LT_p = \{Lt_1^p, Lt_2^p, Lt_3^p,..., Lt_m^p\}$ are the latency times for legitimate users and impostor users respectively, and m is the number of users. The next few sections discuss the latency times discretization mechanisms.

3.1. Discretization Latency Times

This section presents a general method for discretizing latency times. The discretized Times() function shown in Algorithm 2 maps each Lt_i vector to Discretized String (DS_i). Algorithm 2 shows that if the time gap between two consecutive strokes is equal or larger than a specified threshold (λ) then the equivalent symbol *S*, otherwise it is *F*. Lt_i stores the sequence of *F/S* for each password. For example, if $DS_i = \{F,S\}$, then user *i* has a password of 3 characters length and the latency time between the first two characters is *F*, and *S* between the second and third characters.Since people may have different typing styles, deciding on a proper λ value is not trivial.

Algorithm 1: captureLatency()

```
j = 0
Key = get_current_key()
T_Key = T(Key)
while (Key <>Key_Enter) do
        Key = get_current_key()
        t_current_key = T(Key)
```

```
        Lti[j] = t_current_key – t_Key
        t_Key = t_current_key
        j++
end while
returnLti
```

Algorithm 2: discretizedTimes()

```
Require: λ, Lti
for j = 0 to n - 1 do
        If Lti[j] >= λ
                DSi[j] = S
        else
                DSi[j] = F
        end if
end for
returnDSi
```

The next few sections briefly introduce the local threshold based-mechanisms.

3.2. Discretization of Latency Times Using Local Thresholds

This section discusses three different mechanisms for classifying local latency times for each user independently of other users. A local threshold value is determined for each user using his/her password typing style at the sign-up time. The methods are: average, median and min-max.

3.2.1. Latency Times Discretization Using Average

Latency times are classified based on the average latency time of each user, i.e., the collective behavior of all users are not considered. Once a user finishes entering his/her password, the authentication system calculates the average latency time (i.e., λ) from the latency times of the keyed password characters and determines the discrete symbol for each latency time. The algorithm used here is similar to Algorithm 2 except that the value of λ here is the average latency time. The experimental results regarding using the average method is shown in section 5.2.

3.2.2. Discretization Latency Times Using Median

Once a user finishes entering his/her password, the authentication system finds the median of latency times (i.e., λ) and determines the discrete symbol for each latency time. As mentioned in the previous section, the median algorithm is similar to Algorithm 2 except that the value of λ here is the median latency time. The median is calculated for each user, i.e., the collective behavior of all users are also not considered. The experimental results using the median method is shown in section 5.3.

3.2.3. Discretization of Latency Times Using Min-Max

Once a user finishes entering his/her password, the authentication system uses Algorithm 3 to discretize the latency times.

Algorithm 3: min-max()

Require: Lt_i

1: for $j = 0$ to $(n – 1)/2$ do
2: $max\_pos = findMax(Lt_i)$
3: $min\_pos = findMin(Lt_i)$
4: $DS_i[max\_pos] = S$
5: $DS_i[min\_pos] = F$
6: $Lt_i[max\_pos] = -1$
7: $Lt_i[min\_pos] = -1$
8: end for
9: return DS_i

The experimental results when latency times are classified based on the min-max method are presented in 5.4. The min-max algorithm requires several passes to assign F or S for each latency time. In each pass, the minimum latency time of the array of latency times is assigned F and the maximum latency time is assigned S. Each pass ignores the positions of the latency times that were already classified into either F or S.

4. Experimental Methodology

Empirical experiments are executed to test the proposed password hardening mechanisms. A prototype system is programmed to allow users to sign-up/sign-in and used to collect the required data, see Figure 1. The experiments are divided into three parts, the first one allows legitimate users to signup in which the latency times are collected. The second part allows the legitimate users to sign-in and data are collected. The third part allows the impostor users to sign-in using the usernames the passwords of the legitimate users.

The experiments were performed on two different groups where each group consists of 60 students. The first group was mainly IT students while the second group was mainly Non-IT students. Tables 1 and 2 show the demographic data of the participants. An orientation session is delivered to the participants before starting the experiments. For safety, the legitimate users are told not to use usernames and passwords they have for other systems. At the time of conducting the experiments, the approval by the authors' Institutional Review Board (IRB) for such experiments is not required. Each group of participated are divided into two halves, the first half is considered as legitimate users and the other half is theimpostor users. The legitimate users are trained on the system before recording password data. On average, each user needed about 2-3 trials of signing-up before start collecting password data.

Figure 1. Sign up/sign in system.

Since the legitimate users do not have enough experience for using the system, and in order to improve the consistency in keying their password characters using adopted patterns, the legitimate participants are instructed to write their passwords including the time gaps between the letters of the passwords on a paper. For example, a password "newpassword" with its pattern can be written on a paper as new-pass-wor-d, where each dash represents a certain time gap. Two dashes should have longer time than one dash and so on. This time gap is chosen by legitimate users. For example, each dash may represent the time needed to pronounce the word "*mybook*" with a certain speed. This technique may help users in remembering the rhythm. However, users are not supposed to keep on using this technique in real-life.

Table 1. It-students demographic data.

Gender			**Age**	
Male	**Female**	18-22	23-30	>30
28	32	29	21	10

Table 2. Non-it students demographic data.

Gender			**Age**	
Male	**Female**	18-22	23-30	>30
22	38	35	18	7

In our experiments and the sign-in time, the legitimate users are assumed to key their passwords correctly. We concern here about using the correct adopted keying rhythm of passwords. The experiments were divided into three phases as follows:

1. Legitimate users sign-up
   a) A user *i* enters a username.
   b) The user *i* enters his/her password twice using a chosen adopted rhythm. Algorithms 1 and 2 are called to record DS_{i1} and DS_{i2} for each entered password.
   c) The strings DS_{i1} and DS_{i2} are compared.
   d) If the Hamming Distance (HD) between DS_{i1} and DS_{i2} is less than or equal to 1, a successful signup is considered and the user may proceed to step 2, otherwise, the user returns to step *b* above.
   e) Latency times and the DS_{i2} are stored. The $DS_{i2}$is named the *reference string RS*.
2. Legitimate users sign-in
   a) We requested that each legitimate user to sign-in three times using the same keying pattern he/she adopted at the sign-up time.
   b) Latency times for the sign-in trials are stored.
3. Impostor users sign-in
   a) We gave each impostor user a username and its correct password. The impostor users do not have any information about the keying patterns of the legitimate users.
   b) We request that each impostor user to sign-in three times.
   c) Latency times for the sign-in trials by the impostor users are stored.

At the time of data collection, the initial threshold value was fixed at 150ms, i.e., λ=150. Each of the IT and Non-IT groups is divided into 30 legitimate users and 30 impostor users. Therefore, a total of 90 trials (30 users*3 trials) is registered by the legitimate users in each group. The same apply for the impostor users.

In the rest of this paper, the following abbreviations TP, TN, FP, FN stand for: true positive, true negative, false positive and false negative respectively. For each threshold, a number of performance metrics are calculated: false acceptance rate (FAR)=FP/(FP+TN), false rejection rate (FRR)=FN/(FN+TP), precision=TP/(TP + FP) and recall = TP/(TP +FN).

5. Experimental Results

This section shows the experimental results regarding using local threshold value approach is used to determine the DS_i sequence for each password i. The results of the experiments regarding the global threshold value approach are presented in [31].

5.1. Local Threshold Values-Lab Environment

The experimental results related to local threshold values for discretizing latency times based on Lab environment are presented in this section. Local threshold values can vary depending on the typing style of users. During sign-in, the latency times are classified and compared with the reference ARS. The next three sections show the results for the average, median and min-max mechanisms.

The results presented below are divided into two sets of results. The first set belongs to the IT student group while the second set belongs to the Non-IT student group. Comparisons between the results of the two groups are also provided.

Table 3. Local thresholds experimental results for it students.

Legitimate Users		**Impostor users**
HD	***No. of users***	***No. of users***
H_0	75	1
H_1	9	10
H_2	4	11
H_3	2	22
H_4	1	23
H_5	0	17
H_6	0	6
*H*7	0	0
TP	84	——
FN	6	——
FP	——	11
TN	——	79

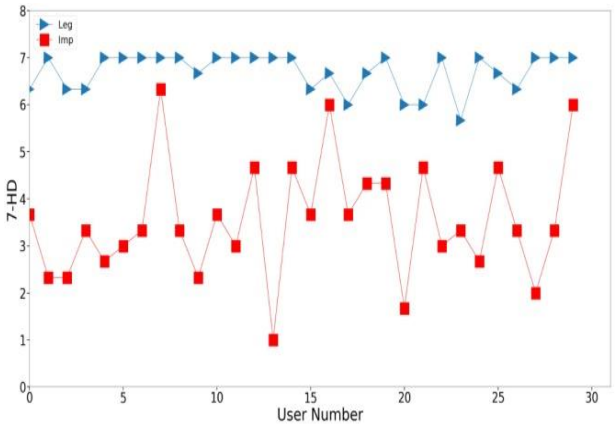

Figure 2. Discretization latency times of 60 IT students (30 Legitimates and 30 impostors) using the average latency time.

5.2. Average Threshold Value

This section shows the experimental results for the average mechanism. Table 3 illustrates the results for 180 trials performed by 60 IT students. Table 3 shows that TP rate=84/90=93.3% if H1 is considered as a valid match. When H0 is only considered, TP rate= 75/90=83.3%. On the other hand, FP rate=11/90= 12.22%, FP rate=1/90=1.11% for H1 and H0 respectively.

Figure 2 shows the results for the thirty legitimate IT students and the thirty impostor IT students in which their 3 trials were averaged. The y−axis represents the number of matches between a given AR and its corresponding ARS (7 minus HD). If we consider a zero HD as a criterion for accessing the system, the true positive rate is 17/30*100%= 56.67%, see Figure 2. On the other hand, when considering 1 HD as a criterion for accessing the system, then the true positive rate is 29/30=96.67%. Finally, Figure 2 shows that at both 0 and 1 HDs, the true negative rate is 100% and 27/30=90% respectively.

The results related to the second group (Non-IT) are presented in Table 4. The results show that TP rate= 83⁄90 = 92.2% if H1 is considered as a valid match which is a bit lower than that of the IT group, see Table 3. However, when H0 is only considered, TP rate=57/90=63.33% which is lower than that (83.8%) of the IT group. On the other hand, FP rate= 27/90=30%, FP rate=8.89% for H1 and H0 respectively. The FP for the Non-IT group is higher than that of the FP for the IT group.

Figure 3 shows the results for the thirty legitimate Non-IT students and the thirty impostor Non-IT studentsin which their 3 trials were averaged.

Table 4. Local thresholds experimental results for non-it students.

Legitimate Users		**Impostor users**
HD	*No. of users*	*No. of users*
H_0	57	8
H_1	26	19
H_2	6	23
H_3	1	20
H_4	0	12
H_5	0	6
H_6	0	2
*H*7	0	0
TP	83	——
FN	7	——
FP	——	27
TN	——	63

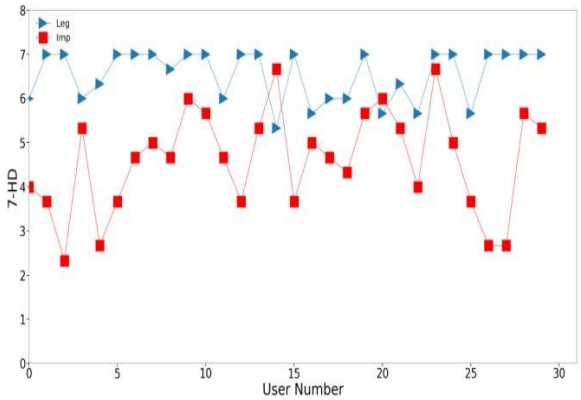

Figure 3. Discretization latency times of 60 Non-IT students (30 Legitimates and 30 impostors) using the average latency time.

If we consider a zero Hamming distance as a criterion for accessing the system, then the true positive rate is 17/30*100%=56.66%, see Figure 3 .On the other hand, when considering 1 Hamming distance as a criterion for accessing the system, the TP rate=24/30=80%. Finally, Figure 3 shows that at both 0 and 1 Hamming distances, the true negative rates are 100% and 4/30=13.3% respectively.

5.3. Median Threshold Value

This section shows the experimental results for the median mechanism used in discretizing latency times. For 180 trials performed by 60 IT users, the TP rate was 64.44 for H0 and 72% for H1. When H0 and H1 are considered, the FP rates were 3.33% and 7.77% respectively.On the other hand, the results of the 180 trials performed by the 60 Non-IT group show that the TP rate was 48.89% for H0 and 61.11% for H1. When H0 and H1 are considered, the FP rates were 23.33% and 43.33% respectively. Figure 4 shows the results for the thirty legitimate IT students and the thirty impostor IT students in which their 3 trials were averaged. If we consider a zero Hamming distance as a criterion for accessing the system, then the true positive rate is

12/30*100%=40%. When considering 1 Hamming distance as a criteria for accessing the system, the true positive rate is 21/30=70%. On the other hand, Figure 4 shows that at 0 Hamming distance, the true negative rate 100%. Finally, at 1 Hamming distance, the true negative rate is 29/30 ≈ 96.7.

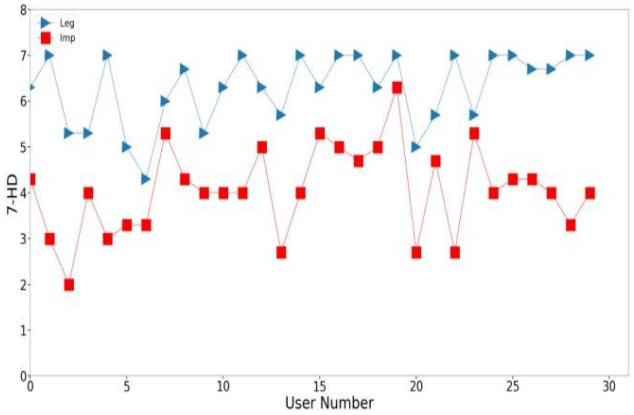

Figure 4. Discretization latency times of 60 IT students (30 Legitimates and30 impostors) using the median latency time.

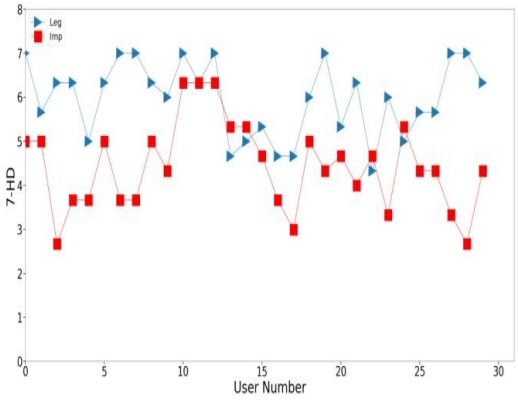

Figure 5. Discretization latency times of 60 Non-IT students (30 Legitimates and 30 impostors) the using median latency time.

For the Non-IT group, Figure 5 shows the results for the thirty legitimate Non-IT students and the thirty impostor Non IT students in which their 3 trials were averaged. If weconsider a zero Hamming distance as a criterion for accessing the system, the true positive rate is 8/30*100%=26.67%. When considering 1 Hamming distance as a criterion for accessing the system, the true positive rate is 17/30=56.67%. On the other hand, Figure 5 shows that at 0 Hamming distance, the true negative rate 100%. Finally, at 1 Hamming distance, the true negative rate is 27/30= 90%.

5.4. Min-Max Method

This section shows the experimental results for the min-max mechanism used in discretizing latency times. For the 180 trials performed by 60 IT group, the TP rate was 71.11% for both H0 and H1. When H0 and H1 were considered, the FP rate was 1.11%. On the other hand, the results of the 180 trials performed by the 60 Non-IT group show that the TP rate was 61.11% for both H0 and H1. When H0 and H1 were considered, the FP rate was 12.22%.

Figure 6 shows the results for the thirty legitimate IT students and the thirty impostor IT students in which their 3 trials were averaged. If we consider a zero Hamming distance as a criterion for accessing the system, the true positive rate was 15/30*100%= 50%. When considering 1 Hamming distance, the true positive rate was 20/30=66.67%. On the other hand, Figure 6 shows that at both 0 and 1 Hamming distances, the true negative rate 100%.

For the Non-IT group, Figure 7 shows the results for the thirty legitimate Non-IT students and the thirty impostor Non-student group performed better than the Non-IT student group in most metrics.

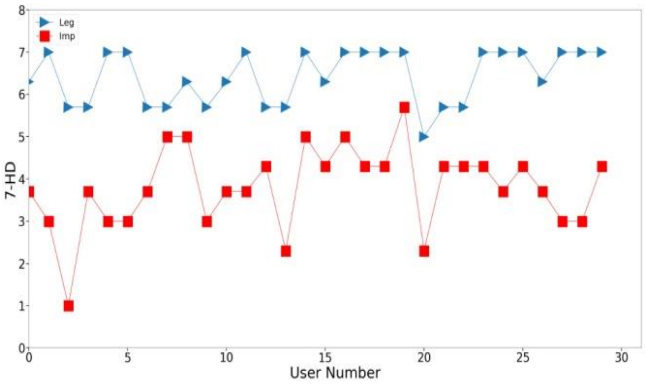

Figure 6. Discretization latency times of 60 IT students (30 Legitimates and 30 impostors) using the min-max latency time.

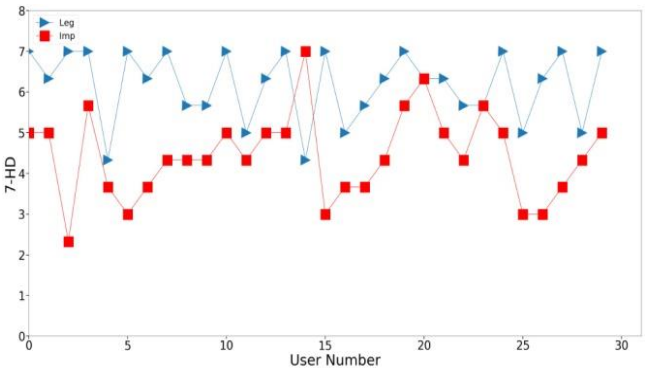

Figure 7. Discretization latency times of 60 Non-IT students (30 Legitimates and 30 impostors) using the min-max latency time.

IT students in which their 3 trials were averaged. If we consider a zero Hamming distance as a criterion for accessing the system, the true positive rate was 40%. When considering 1 Hamming distance, the true positive rate was 63.33%. On the other hand, Figure 7 shows that at both 0 and 1 Hamming distances, the true negative rates were 96.67% and 93.33% respectively.

To summarize the results for local threshold approach, Table 5 shows the results related to average, median and min-max mechanisms for both the IT and Non-IT students.

The (.,.) shown in Table 5 means that (IT result, Non-IT result). The results show that the average mechanism outperformed the other two mechanisms in

both the IT and Non-IT student groups. The reason is that the threshold presented by the average latency times represents the users' patterns more correctly than the median. The min-max method compares between each two latency times, in this case users were not able to keep the relationship between every two latency timesconsistent. On the other hand, all methods were effective in protecting the system form impostor users. Finally, the IT student group performed better than the Non-IT student group.

Table 5. Summary of Results for the Three Local Threshold Methods by both It and Non-It Students.

Metric	Avg H0(%)	Avg H1(%)	Med H0(%)	Med H1(%)	Min-max H0(%)	Min-max H1(%)
TP rate	(83,63)	(92,92)	(71,61)	(71,61)	(50,40)	(67,63)
FN rate	(17,37)	(8,8)	(29,39)	(29,39)	(50,60)	(33,37)
TN rate	(99,91)	(88,70)	(99,88)	(99,88)	(100,97)	(100,93)
FP rate	(1,9)	(12,30)	(1,12)	(1,12)	(0,3)	(0,3)

Table 6. Summary of results for the real-world experiments.

Cat.	H_0	H_1	H_2	H_3	H_4	H_5	H_6	TP rate	TN rate
LAvg	64	24	2	0	0	0	0	97.8%	–
IAvg	0	5	18	24	30	11	2	–	94.4%
LMed	32	16	30	3	1	8	0	53.3%	–
IMed	0	6	19	16	44	4	1	–	93.3%
LMM	53	0	17	8	12	0	0	58.9%	
IMM	1	1	15	10	42	7	14	–	97.8

5.5. Local Threshold Values for Real-World Experiments

This section discusses the results obtained from the realworld experiments. Two IT professionals participated in the experiment for 10 continuous days. The system was installed on their machines and they were asked to login 3 times every day as they would do with any other system such as email systems. After 10 days the data was collected. Their user names and passwords (without the rhythms) were given to other 2 users playing the role of impostors. The two users playing the role of imposer users were asked to log-in to the system 30 times.

Table 6 shows the summary of the results. The first column in the table shows the category of users where L stands for legitimate, I stands for impostor and MM stands for min-max. Again, the average discretizing method proves to be better than the other two methods. It is noted that the results of the realworld experiments outperform the results of the experiments done in lab. The reason is that people in the real-world setting were not under stress. In addition, the IT professional people can perfect the keying rhythm better than other none IT professionals.

Considering the results for the average method in Table 6, the FAR, FRR for H1 are 0.055 and 0.022 respectively. When H0 is used as a reference criterion, the FAR, FRR are 0 and 0.29 respectively. The work presented in [18] used a k-nearest neighbor approach to classify users keystroke dynamics profiles with FAR, FRR are 0.045 and 0 respectively. However, the authentication speed may take 16s and that time increases with the increase of the database size. This verification time may reduce the system usability. A more recent study [23] shows through extensive empirical experimentations that the authentication performance was highly dependent on the size of both reference and test keystrokes. In our proposed authentication mechanism, these factors are irrelevant.

It is noteworthy to state that the comparison between the FAR/FRR obtained in this study and the FAR/FRR obtained in Keystroke Dynamics algorithms is not fair or useful. In this paper authentication is achieved through two secrets that the user has to recall: the password sequence and the password rhythm. In KD users memorize the password and nothing else.

6. Practicality of the Mechanism

This section discusses the issues related to using such a password hardening method in real computer systems. The issue that can be argued against using such mechanism is whether remembering and repeating the adopted keying rhythm of a password is practical and what is the cognitive load associated with it. First of all, users need to practice the proposed method before it becomes effective. There are some techniques that can be used to make the remembering process easy. One method is to ask the user to select a certain rhythm for the password and say it as a short song then type it on the keyboard while synchronizing their typing speed with singing the words of the song. Similar approach is also presented in [7]. Moreover, the work presented in [7] shows that the uniqueness and consistency of the typing style improve the learning outcomes of classifiers.

Another technique that may assist users to remember the adopted keying style is to divide their passwords into several parts then to type each part using a certain speed and wait for some time then type the second one with a different speed etc. This method is similar to the technique of dividing a phone number into a number of sections to help memorizing the number [8].

The initial performed experiments indicate that a good percentage of the students who participated in the experiments demonstrate that they can learn to use the proposed approach after few trials. Moreover, individuals with strong IT background performed better than the individuals with Non-IT background. In general, many participants showed their interest in using this authentication mechanism since it provides a better security for textual passwords.

One more issue that can be raised here is whether users can manage using this technique with different accounts, and which is better, to have a longer

password or having a shorter password associated with a rhythm? The answer to such questions are left for future work.

A final note is that the proposed authentication mechanism may protect systems from impostor users even if they have the correct passwords because they do not know the right keying patterns of passwords. In addition, the proposed password hardening mechanism can have other security applications such as detecting password file theft [30].

7. Conclusions and Future Work

Authentication systems are essential part of any information system. As textual passwords authentication mechanism is stillwidely used, the idea presented in this paper discusses theissue of hardening textual passwords. A number of techniquesto discretize the latency times for password hardening arepresented. The average, median and min-max are used todiscretize latency times for password hardening.
Two discrete symbols, S for slow and F for fast are usedto represent a password rhythm. A threshold value is used tomap the latency time into either S or F. If the latency timeis larger than or equal a certain threshold value, the latencytime is registered as to S, otherwise it is mapped to F.

To test the proposed method, a prototype is programmedand used to collect data from participants. The experimentaldata are collected from two settings: real-world and Lab. TheLab setting includes university students studying Information Technology (IT) and a non-IT group from the same university. On the other hand, the real-world experiment includes informationtechnology professional members. The experimentalresults show that the proposed password hardening methodis effective in protecting impostor users from accessing thesystem. In addition, the average descritization method showsbetter results when compared with the median and min-maxmethods. Finally, the experimental results of the real-worldsetting experiments highly support both the practicality of theproposed password hardening mechanism and its effectiveness.

As a future work, the vulnerability of the proposed systemto attacks should be investigated since the sound emanated bythe keyboard when typing the password may provide useful information about the elapsed time between the pressed keys. In addition, we need to investigate the use of the proposedauthentication mechanism in mobile applications.

Acknowledgment

This research is funded by the deanship of scientific research at Zarqa University, Jordan.

References

[1] Al-Rahmani A., "An Enhanced Classifier for Authentication in Keystroke Dynamics Using Experimental Data," PhD Thesis, Middle East University, 2014.

[2] Alsulaiman F. and El Saddik A., "Three-Dimensional Password forMore Secure Authentication," *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 9, pp. 1929-1938, 2008.

[3] Bergadano F., Gunetti D., and Picardi C., "Identity Verification through Dynamic Keystroke Analysis," *Intelligent Data Analysis*, vol. 7, no. 5, pp. 469-496, 2003.

[4] Bonissi A., Labati R., Perico L., Sassi R., Scotti F., and Sparagino L.,"A Preliminary Study on Continuous Authentication Methods for Photo Plethysmographic Biometrics," *in Proceedings of IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS)*, pp. 28-33, 2013.

[5] Chang T., Peng C., Tsai C., Chen Y., and Cheng P., "Personalized Rhythm Click Based Authentication System Improvement using a Statistical Classifier," *in Proceedings of 2nd International Conference on Information Communication and Management*, pp. 39-43,2012.

[6] Cho S., Han C., Han D., and Kim H., "Web-Based Keystroke Dynamics Identity Verification Using Neural Network," *Journal of Organizational Computing and Electronic Commerce*, vol. 10, no. 4, pp. 295-307, 2000.

[7] Cho S. and Hwang S., "Artificial Rhythms and Cues for Keystroke Dynamics Based Authentication," *in Proceedings of the International Conference on Advances in Biometrics*, Hong Kong, pp. 626-632, 2006.

[8] Conklin A., Dietrich G., and Walz D., "Password-Based Authentication: A System Perspective," *in Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, Big Island, pp. 1-10, 2004.

[9] Dasgupta D., Roy A., and Nag A., *Advances in User Authentication*, Springer International Publishing Cham, 2017.

[10] De Angeli A., Coventry L., Johnson G., and Renaud K., "Is a Picture Really Worth A Thousand Words? Exploring the Feasibility of Graphicalauthentication Systems," *International Journal of Human Computer Studies*, vol. 63, no. 1-2, pp. 128-152, 2005.

[11] De Magalhaes S., Revett K., and Santos H., "Password Secured Sites-Stepping Forward with Keystroke Dynamics," *in Proceedings of International Conference on Next Generation*

Web Services Practices (NWeSP'05), Seoul, South Korea, pp. 6, 2005.

[12] Fayyadh B., Mansour K., and Mahmoud K., "New Pass Word Authentication Mechanism Using 2d Shapes," *in Proceedings of 8th International Conference on Computer Science and Information Technology*, pp. 113-118, 2018.

[13] Fazal K. and Syed A., "Blockchain Authentication Mechanism For Securing Internet of Things," *Pakistan Journal of Engineering and Technology*, vol. 3, no. 2, pp. 51-58, 2020.

[14] Fed Trade Commission. Identity Theft, https://www.ftc.gov/news-events/media-resources/identity-theft, Last Visited, 2019.

[15] Florˆencio D., Herley C., and Oorschot P., "An Administrators Guide to Internet Password Research," *in Proceedings of 28th Large Installation System Administration Conference*, Seattle, pp. 35-52, 2014.

[16] Guo Y., Zhang Z., and Guo Y., "Optiwords: A New Password Policy for Creating Memorable And Strong Passwords," *Computers and Security*, vol. 85, pp. 423-435, 2019.

[17] Haider S., Abbas A., and Zaidi A., "A Multi-Technique Approach for User Identification Through Keystroke Dynamics," *in Proceedings of IEEE International Conference on Systems, Man, and Cybernetics*, Nashville, pp.1336-1341, 2000.

[18] Hu J., Gingrich D., and Sentosa A., "A K-Nearest Neighbor Approach for User Authentication Through Biometric Keystroke Dynamics," *in Proceedings of IEEE International Conference on Communications*, Beijing, pp. 1556-1560, 2008.

[19] Jadhao P. and Dole L., "Survey on Authentication Password Techniques," *International Journal of Soft Computing and Engineering*, vol. 3, no. 2, pp. 67-68, 2013.

[20] Jain A. and Nandakumar K., "Biometric Authentication: System security and User Privacy," *Computer*, vol. 45, no. 11, pp. 87-92, 2012.

[21] Janakiraman R. and Sim T., "Keystroke Dynamics in A General Setting," *in Proceedings of International Conference on Biometrics*, Seoul, pp. 584-593, 2007.

[22] Janik L., Chuda D., and Burda K., "Sgfa: A Two-Factor Smartphone Authentication Mechanism Using Touch Behavioral Biometrics," *in Proceedings of the 21st International Conference on Computer Systems and Technologies*, New York, pp. 35-42, 2020.

[23] Kang P. and Cho S., "Keystroke Dynamics-Based User Authentication using Long and Free Text Strings from Various Input Devices," *Information Sciences*, vol. 308, pp. 72-93, 2015.

[24] Kim J., Kim H., and Kang P., "Keystroke Dynamics-Based User Authentication Using Freely Typed Text Based on User-Adaptive Feature Extraction and Novelty Detection," *Applied Soft Computing*, vol. 62, pp. 1077-1087, 2018.

[25] Klein D., "Foiling the Cracker: A Survey of, and Improvements to, Password Security," *in Proceedings of the 2nd USENIX Security Workshop*, pp. 5-14, 1990.

[26] Lashkari A., Farmand S., Zakaria O., and Saleh R., "Shoulder Surfing Attack in Graphical Password Authentication," *International Journal of Computer Science and Information Security*, vol. 6, no. 2, pp. 145-154, 2009.

[27] Lau S. and Maxion R., "Clusters and Markers for Keystroke Typing Rhythms," *LASER*, pp. 1-10, 2014.

[28] Liebers J. and Schneegass S., "Introducing Functional Biometrics: Using body-Reflections as A Novel Class of Biometric Authentication Systems," *in Proceedings of Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, New York, pp. 1-7, 2020.

[29] Mahmoud K., "Elastic Password: A New Mechanism for Strengthening passwords Using Time Delays between Keystrokes," *in Proceedings of the 8th International Conference on Information and Communication Systems*, Irbid, 2017.

[30] Mahmoud K., Mansour K., and Makableh A., "Detecting Password File Theft using Predefined Time-Delays between Certain Password Characters," *Journal of Telecommunications and Information Technology*, vol. 4, no. 4, pp. 101-108,

[31] Mansour K., "A New Mechanism for Textual Password Hardening Using Adopted Typing Rhythm," *in Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*," New York, pp. 1-8, 2018.

[32] Maxion R. and Killourhy K., "Keystroke Biometrics with Number Pad Input," *in Proceedings of the International Conference on Dependable Systems and Networks*, Chicago, pp. 201-210, 2010.

[33] Mehmood R. and Selwal A., "Polynomial Based Fuzzy Vault Technique for Template Security in Fingerprint Biometrics," *The International Arab Journal of Information Technology*, vol. 17, no. 6, pp. 926-934, 2020.

[34] Monrose F., Reiter M., and Wetzel S., "Password Hardening Based on keystroke Dynamics," *in International Journal of Information Security*, vol. 1, pp. 69-83, 2002.

[35] Morales A., Falanga M., Fierrez J., Sansone C., and Ortega-Garcia J., "Keystroke Dynamics Recognition based on Personal Data: A

Comparative Experimental Evaluation Implementing Reproducible Research," *in Proceedings of IEEE 7th International Conference on Biometrics: Theory, Applications and Systems*, Arlington, pp. 1-6, 2015.

[36] Nandy T., Idris M., Noor R., Kiah L., Lun L., Jumaat N., Ahmedy I., Ghani N., and Bhattacharyya S., "Review on Security of Internet of Things Authentication Mechanism," *IEEE Access*, vol. 7, pp. 151054-151089, 2019.

[37] O'Gorman L., "Comparing Passwords, Tokens, and Biometrics for User Authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021-2040, 2003.

[38] Pietron A. and Han T., "A Case Study of Graphical Passwords in Achinese University," *in Proceedings of Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization*, New York, pp. 175-180, 2020.

[39] Raul N., Shankarmani R., and Joshi P., "A Comprehensive Review of keystroke Dynamics-Based Authentication Mechanism," *in Proceedings of International Conference on Innovative Computing and Communications*, Singapore, pp. 149-162, 2020.

[40] Roth J., Liu X., Ross A., and Metaxas D., "Biometric Authentication Viakeystroke Sound," *in Proceedings of International Conference on Biometrics*, Madrid, pp. 1-8, 2013.

[41] Sung K. and Cho S., "GA SVM Wrapper Ensemble for Keystroke Dynamics Authentication," *in Proceedings of International Conference on Biometrics*, Hong Kong, pp. 654-660, 2006.

[42] Skračić K., Pale P., and Kostanjčar Z., "Authentication Approach Using Onetime Challenge Generation Based on User Behavior Patterns Captured Intransactional Data Sets," *Computers and Security*, vol. 67, pp. 107-121, 2017.

[43] Spillane R., "Keyboard Apparatus for Personal Identification," *IBM Technical Disclosure Bulletin*, vol. 17, pp. 3346, 1975.

[44] Subashini S. and Kavitha V., "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1-11, 2011.

[45] Teh P., Yue S., and Teoh A., "Feature Fusion Approach on Keystroke Dynamics Efficiency Enhancement," *International Journal of Cyber-Security and Digital Forensics*, vol. 1, no. 1, pp. 20-31, 2012.

[46] Zhong Y. and Deng Y., *Recent Advances In User Authentication Using Keystroke Dynamics Biometrics*, Science Gate Publishing, 2015.

[47] Zhong Y., Deng Y., and Jain A., "Keystroke Dynamics for user Authentication," *in Proceedings of Computer Vision and Pattern Recognition Workshops*, Providence, pp. 117-123, 2012.

[48] Zimmermann V. and Gerber N., "The Password Is Dead, Long Live The password A Laboratory Study on User Perceptions of Authentication Schemes," *International Journal of Human-Computer Studies*, vol. 133, pp. 26-44, 2020.

Khalid Mansour received his PhD degree in computer science from Swinburne University of Technology (Australia) in 2014. In addition, he earned the MBA from Jordan University in 2008. He is an associate professor in artificial intelligence and his research interests are in automated negotiation in multi-agent systems, machine learning and information security. He is currently the head of department of data science and artificial intelligence at Zarqa University/Jordan.

Khalid Mahmoud received his BSc degree in Computer Science from Jordan University on June 1992, MSc degree in Computer Science (Artificial Intelligence) from Jordan University on 1998 and PhD degree in Print Security and Digital Watermarking from Loughborough University (UK) on 2004. This was followed by academic appointments at ZARQA Private University as an assistance Professor in computer Science. On 2018 he joined Princess Sumaya University as an academic staff in computer science department. His areas of interest include Information security, Digital watermarking, Image forgery detection, AI and Arabic language processing.