مجلة العلوم البحثة والتطبيقية
Journal of Pure & Applied Sciences
www.Suj.sebhau.edu.ly ISSN 2521-9200
Received 07/05/2019 Revised 22/08/2019 Published online 17/11/2019

المصادقة المستمرة للمستخدم على أساس ديناميكية المفاتيح
(تطبيق على الكلمات العربية شائعة ونادرة الاستخدام)

*فاطمة القاضي و عمر شيبه
قسم الحاسوب– كلية العلوم– جامعة سبها، ليبيا
*للمراسلة: fa.alqadhi@sebhau.edu.ly

الملخص تعتبر المصادقة المستمرة Continuous Authentication احد اساليب المصادقة التي ظهرت لحل مشكلة التحقق من ما إذا كان من يستخدم النظام المصادق عليه هو ذاته من لحظة تسجيل الدخول الي لحظة تسجيل الخروج، وتعتبر ديناميكية المفاتيح Keystroke Dynamics احد اساليب المصادقة المستمرة التي يمكن استخدامها في المصادقة اما في شكل النص الثابت fixed text او النص الحر free text . لهذا تهدف هذه الورقة لدراسة امكانية استخدام كلمات عربية محددة في مصادقة المستخدم مصادقة مستمرة على اساس ديناميكية المفاتيح، وكذلك دراسة الفروق بين اداء نظام المصادقة عند استخدام كلمات شائعة الاستخدام في المصادقة وادائه عند استخدام كلمات نادرة الاستخدام في المصادقة. تم في هذه الدراسة تطبيق احد خوارزميات المصادقة المستمرة على أساس ديناميكية المفاتيح على عشر كلمات عربية من الكلمات شائعة الاستخدام في رسائل البريد الالكتروني e-mail, وثلاثة كلمات عربية نادرة الاستخدام، حيث تم استخدام اربعة من خصائص التوقيت لاستخراج الميزات من نمط كتابة المستخدمين على لوحة المفاتيح، و لتصنيف بيانات المستخدمين تم استخدام أحد مقاييس المسافة من النهج الإحصائي وهو مقياس مسافة مانهاتن الموزونة Scaled Manhattan distance والعتبة الفردية Individual threshold ومستوى الثقة trust level وقيمة القفل Tlockout . وقد أظهرت النتائج أنَّه من الممكن مصادقة المستخدمين مصادقة مستمرة استناداً إلى ديناميكية مفاتيح اللغة العربية للنص الثابت.

الكلمات المفتاحية: القياسات الحيوية، المصادقة الثابتة، المصادقة المستمرة، ديناميكية المفاتيح، مصادقة المستخدم.

Continuous authentication for the user based on Keystroke Dynamics (Applied to commonly and rarely used Arabic words)

*F. Algadi , O. Shiba
Computer science department, college of science/Sebha university, Libya
*Corresponding author: fa.alqadhi@sebhau.edu.ly

Abstract Continuous Authentication considered as one of the authentication methods that has been emerged to solve the problem verifying whether who is using the system is the same one from the moment of login to the moment of logout, Keystroke Dynamics is one of the continuous authentication methods that can be used for authentication either in the form of fixed text or free text. The purpose of this paper is to study the possibility of using specific Arabic words to authenticate the user continuous authentication based on Keystroke Dynamics, as well as to examine the differences between the performance of the authentication system when using the commonly used words in authentication and its performance when using rarely used words in authentication. In this study, one of the continuous authentication algorithms based on Keystroke Dynamics has been applied to ten Arabic words of commonly used words in e-mail, and three Arabic words which are rarely used, where four of the timing characteristics were used to extract the features of the typing style of users on the keyboard. To classify user's data, a measure of distance from the statistical approach, which is the Scaled Manhattan distance measure, Individual threshold, trust level and Tlockout were used. The results have shown that it is possible to authenticate users using continuous authentication based on the Arabic Language Keystroke Dynamics of fixed text .

Keywords: Biometrics, Continuous Authentication, Keystroke Dynamics, Static Authentication, User Authenticate.

المقدمة

أثار الانتشار المتزايد للخدمات الالكترونية عن بُعد عبر الإنترنت مطلباً للتقنيات التي يمكن من خلالها التحقق من هوية المستخدمين المزعومة عن بُعد .يتم عادة تنفيذ مصادقة المستخدم بشكل ثابت عند لحظة دخوله للنظام "مرة واحدة فقط" لتحقيق هذا المطلب، وهذا لا يضمن ان من يستخدم النظام هو ذاته أثناء الجلسة الكاملة، في حين ان المصادقة المستمرة Continuous Authentication(CA) تسعى إلى معالجة أوجه القصور في المصادقة الثابتة Static Authentication(SA) من خلال رصد هوية المستخدم أثناء الجلسة الكاملة [1]، وتعتبر القياسات الحيوية احد اساليب المصادقة الناجحة التي يمكن استخدامها في

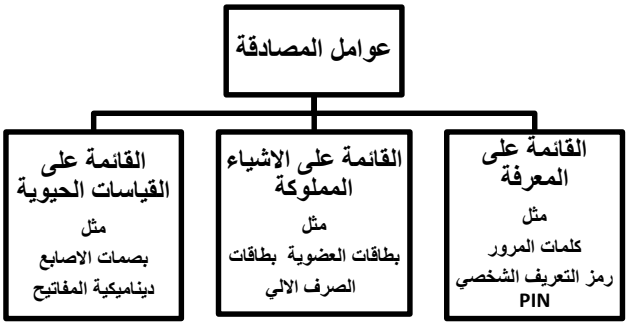
شكل مصادقة ثابتة او مستمرة، ومنها ديناميكية المفاتيح التي تعتبر احد القياسات الحيوية السلوكية المعبّرة عن النمط الذي يقوم المستخدم من خلاله بكتابة الأحرف أو الأرقام على لوحة المفاتيح، وتستخدم لتحديد هوية الشخص لأنها تشبه خط اليد أو التوقيع، ويتم استخدامها بشكل متزايد لمصادقة المستخدم لكونها سهلة التنفيذ حيث تعتبر لوحات المفاتيح من أجهزة الإدخال الشائعة التي يمكن العثور عليها بسهولة على أجهزة الكمبيوتر والهواتف وأجهزة الصرف الآلي وغيرها [2].

دراسات ذات علاقة

يوجد العديد من الدراسات التي تهدف إلى دراسة فاعلية استخدام تقنية ديناميكية المفاتيح لمصادقة المستخدمين على منصات سطح المكتب. فعلى سبيل المثال اقترحت [3] خوارزمية لتطبيق ديناميكية المفاتيح باعتبارها مصادقة مستمرة في مجال البريد الإلكتروني لبعض الكلمات الأكثر استخداما في رسائل البريد الالكتروني باللغة الانجليزية و قد تم استخدام برنامج GREYC-Keystroke المتاح للتجربة على الانترنت في استخراج ميزات نمط الكتابة للمشتركين وتنفيذ التجربة وتم الحصول على معدل EER منخفض، بينما كانت دراسة أخرى [4] تنفيذ ديناميكية المفاتيح كنظام مصادقة ثابت لتطبيق سطح مكتب تم بنائه باستخدام Microsoft Visual Studio 2010 حيث يطلب من المشاركين في التجربة كتابة جملة قصيرة ثابتة عشر مرات في مرحلة التدريب وفي مرحلة المصادقة يتم مقارنة الميزات المستخرجة منها مع ميزات الكتابة الحالية لذات الجملة، استخدمت هذه الدراسة زمن الكمون و زمن الرحلة و الزمن الإجمالي لكلمة المرور كميزات لديناميكية المفاتيح والنهج الاحصائي للتصنيف واكدت هذه الدراسة فاعلية تنفيذ ديناميكية المفاتيح على منصة سطح المكتب. وتهدف دراسة أخرى [5] إلى الإجابة عن السؤال "هل يمكن لمنتحل أن يتعلم خصائص الكتابة لشخص ما؟" تم فيها إجراء تجربتين كان الغرض من الاولى هو اختبار مقاييس المسافة المختلفة لاختيار أفضل مقياس مسافة واستخدامه في التجربة الثانية التي كان الغرض منها الإجابة على سؤال البحث وقد أظهرت نتائج هذه التجارب قدرة المنتحلين على تقليد نمط الكتابة للمستخدمين الحقيقين عند معرفتهم معلومات كافية عن خصائص كتابتهم ، ولكن ليس من السهل على نحو مقلق. كما أظهرت هذه الدراسة أن ديناميكيات المفاتيح هي طريقة مصادقة ثابتة آمنة جداً عند دمجها مع كلمة مرور.

المصادقة

هي عملية التحقق من هوية شخص ما أو شيء ما [6]. تشكل آليات المصادقة عادةً خط الدفاع الأول في نظم أمن الحاسوب، وتُعد واحدة من أهم الجوانب وأكثرها تحدياً للتحكم في الوصول غير المصرح به للنظم [1]. ، حددت الأبحاث في مجال امن النظم أنه من أجل تحديد هوية المستخدم بشكل قاطع، يفضل استخدام اثنين على الأقل من عوامل المصادقة، والافضل استخدام العوامل الثلاثة معا [6]. يوضح الشكل1 عوامل المصادقة الثلاثة .



شكل1: يوضح عوامل المصادقة

القياسات الحيوية

تشير القياسات الحيوية إلى بعض الخصائص الفسيولوجية أو السلوكية التي ترتبط بشكل فريد بشخص معين، وتعدّ هذه الخصائص مميزة للغاية ويمكن استخدامها للتمييز بين الأفراد المختلفين [7]. توجد فئتان لتقنيات القياسات الحيوية وهي [8] :

- **البيولوجية**

تعتمد هذه التقنية على معرفة الفرد من خلال تحليل البيانات البيولوجية المرتبطة به (على سبيل المثال DNA ، بصمات الاصابع، شبكية العين).

- **السلوكية**

تعتمد هذه التقنية على معرفة الفرد من خلال تحليل سلوكه أثناء قيامه بمهمة محددة (على سبيل المثال التوقيع ، الصوت ، ديناميكية المفاتيح).

اقترحت المنظمة الدولية للمعايير ISO / IEC 19795-1 عدة مقاييس إحصائية لتقييم اداء النظم المبنية على القياسات الحيوية (النظم البيومترية) اهمها [7] :

- **معدل القبول الخاطئ** (FAR)

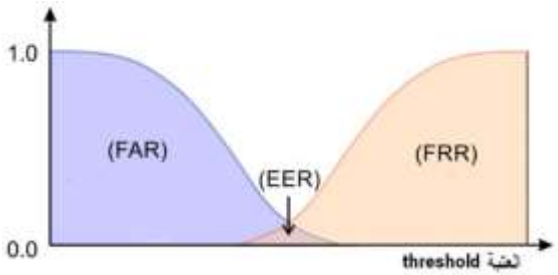
يشير FAR إلى النسبة المئوية بين المستخدمين غير المصرح لهم الذين تم قبولهم خطأ مقابل إجمالي عدد المنتحلين الذين يحاولون الوصول إلى النظام [9]، ويدل FAR المنخفض على قبول عدد منتحلين أقل.

- **معدل الرفض الخاطئ** (FRR)

يشير FRR إلى النسبة المئوية بين المستخدمين الحقيقيين الذين تم رفضهم خطأً مقابل إجمالي عدد المستخدمين الحقيقيين الذين يصلون إلى النظام [9]، ويدل FRR المنخفض على رفض أقل ووصول أسهل للنظام من قبل المستخدم الحقيقي.

- **معدل الخطأ المتساوي** (EER)

يشير EER إلى النقطة التي يتقاطع عندها FAR مع FRR ويمكن الحصول عليها بسهولة من خلال نقطة تقاطع منحنيات FAR و FRR كما هو مبين بالشكل2. ويدل EER المنخفض على ارتفاع دقة نظام المصادقة البيومترية.



شكل2: يوضح مقاييس اداء النظم البيومترية FAR و FRR و EER

المصادقة الثابتة و المصادقة المستمرة

المصادقة الثابتة هي آلية تحقق من هوية المستخدم عند نقطة الدخول فقط للجلسة أي لحظة تسجيل الدخول [10]. في حين تشير المصادقة المستمرة الى آلية تحقق من هوية الفرد بشكل متكرر طوال مدة الجلسة [11] (من حين تسجيل الدخول الى حين تسجيل الخروج). وفي حالة استخدام المصادقة الثابتة عندما يتحرك المستخدم بعيداً عن جهازه ليأخذ استراحة دون تسجيل الخروج ، فإن المستخدم يكون عرضة للتغير حيث يمكن ان يأخذ المنتحل مكان المستخدم المصادق عليه ويعمل أي اجراءات داخل النظام بهوية المستخدم، هذا يمكن أن يثبت أنَّه ضعف أمني خطير في أنظمة الأمان العالي [10]، ولمعالجة هذه المشكلة يحتاج النظام إلى التحقق باستمرار من مطابقة هوية المستخدم وبذلك سيظل النظام آمنا حتى إذا نسي المستخدم تسجيل الخروج من النظام بعد انتهاء جلسته وهذا هو هدف المصادقة المستمرة [12].

ديناميكية المفاتيح

تشير ديناميكية المفاتيح إلى عملية قياس نمط الكتابة البشرية على الأجهزة الرقمية على سبيل المثال لوحة مفاتيح الكمبيوتر أو الهاتف المحمول أو لوحة شاشة الهواتف المحمولة التي تعمل باللمس. يتم إنشاء شكل من اشكال التوقيعات الرقمية من خلال التفاعل البشري مع هذه الأجهزة، ولوحظ أنَّ نمط ضغط المفاتيح له نفس العوامل العصبية الحيوية التي تجعل التوقيع اليدوي فريدا و هذه التوقيعات غنية بالصفات المعرفية وتحمل إمكانات هائلة للاستخدام باعتبارها معرّفا شخصياً [13]. يمكن استخدام ديناميكية المفاتيح كأسلوب مصادقة ثابتة من خلال رصد نمط كتابة المستخدم لاسم المستخدم وكلمة المرور او كأسلوب مصادقة مستمرة اما باستخدام النص الثابت وفيه يتم منح المستخدم نصاً محدداً مسبقاً (عادة ما تكون نصوص قصيرة او مجموعة كلمات منفصلة) ويطلب منه كتابة هذا النص اثناء مرحلة التدريب لبناء قالب المقارنة وأثناء مرحلة المصادقة يتم مقارنة عينة الكتابة الجديدة بالقالب المخزن مسبقا لذات المستخدم، أو باستخدام النص الحر وفيه يُطلب من المستخدم كتابة نصوص طويلة تحاكي فكرة النص الحر أو يُترك المستخدم ليكتب ما يشاء دون قيود في كل من مرحلة التجميع ومرحلة المصادقة.

طريقة البحث

شارك في تجارب هذه الورقة 21 مشارك من الناطقين باللغة العربية ولديهم اختلاف في مهارات الكتابة على لوحة المفاتيح. قدم المشاركين عينات الطباعة باللغة العربية على اجهزة الحاسوب الخاصة بهم وذلك من خلال تطبيق انترنت تفاعلي تم تصميمه لهذا الغرض باستخدام استراتيجية النشر الهجين ، حيث تم تنفيذ التطبيق في جانب العميل باستخدام HTML,CSS, JavaScript في حين تم استخدام لغة برمجة تطبيقات الويب PHP وقاعدة البيانات MySQL على جانب الخادم.

1. **استخراج الميزات وانشاء قالب المقارنة**

لاستخراج الميزات تمَّ اختيار عشر كلمات عربية من الكلمات شائعة الاستخدام في رسائل البريد الالكتروني e-mail وهي (***مرحبا، السلام عليكم، تحية طيبة، شكرا، اما بعد، جيد، الى اللقاء، مع السلامة، بخير، كيف الحال***) والسبب وراء اختيار هذه الكلمات هو أنَّ نمط الكتابة لها مستقر نسبياً نظراً لأن المستخدمين اعتادوا كتابتها، وثلاثة كلمات عربية نادرة الاستخدام وهي (***حجية، متضادة، مستشفى***) تم اختيارها نظراً لأن حروفها تقع في مواقع مختلفة على لوحة المفاتيح.

يُطلب في مرحلة التدريب من الاشخاص المستهدفين التسجيل في التطبيق عن طريق كتابة اسم مستخدم وكلمة مرور من اختيارهم وعنوان البريد الالكتروني الخاص بهم كما موضح بالشكل3 ومن ثم كتابة كل كلمة من الكلمات قيد الدراسة عشرة مرات بطريقة طبيعية كما موضح بالشكل4.

شكل3: يوضح واجهة مرحلة التسجيل في التطبيق

شكل4: يوضح واجهة مرحلة بناء قالب المقارنة

استخدمت في هذه الدراسة ميزات ديناميكية المفاتيح الزمنية المستخدمة في [3] نظراً لأنَّ هذه الميزات كافية لتمييز سلوك الكتابة (ديناميكية المفاتيح) ، وهذه الميزات هي:

PP (Press-Press) : هي الفترة الزمنية ما بين الضغط على مفتاحين متتاليين.

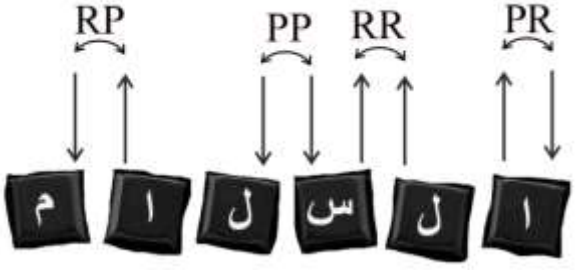
PR (Press-Release) : هي الفترة الزمنية بين الضغط على وافلات مفتاح واحد.

RP (Release- Press) : هي الفترة الزمنية بين إفلات مفتاح والضغط على آخر.

RR (Release -Release) : هي الفترة الزمنية بين إفلات مفتاحين متتاليين.

وقد تم قياس هذه الميزات بالملي/ثانية m/s، ويوضح الشكل5 مثال لهذه الميزات عندما يدخل المستخدم كلمة "السلام".

ومن ثم تم انشاء قالب مقارنة لكل شخص مستهدف في التجربة، وذلك من خلال إيجاد المتوسط الحسابي لكل ميزة من الميزات الأربع للعشر ادخالات لكل كلمة على حدة.



شكل5: ميزات ديناميكية المفاتيح لإدخال كلمة " السلام"

2. مرحلة المصادقة

في نظم المصادقة المستمرة المبنيَّة على ديناميكية المفاتيح يتم تحديد قبول أو رفض وصول المستخدمين للنظام بناء على نمط طباعة المستخدم على لوحة المفاتيح. ولن يتم رفض المستخدم من قبل النظام بناءً على مفتاح واحد فقط تم ضغطه بطريقة خاطئة، بل سيقوم النظام برفض المستخدم عند استمراره في الطباعة بطريقة بعيدة عن قالب المقارنة على مدى فترة زمنية. وبمجرد الانتهاء من مرحلة استخراج الميزات لتمثيل خصائص الكتابة للمستخدم، تبدأ عملية التصنيف لغرض المصادقة واثبات الهوية. وقد تم تطبيق العديد من طرق التصنيف في الدراسات البحثية في هذا المجال وكان أهمها النهج الإحصائي وطرق تعلم الآلة [13] ومن أكثر الطرق استخداما طريقة قياس المسافة من النهج الاحصائي، حيث يتم قياس المسافة بين نمط الكتابة الحالي للمستخدم لتحديد التشابه / الاختلاف بينه وبين قالب المقارنة المخزّن بقاعدة البيانات. هناك العديد من مقاييس المسافة اهمها مقياس المسافة الاقليدية Euclidean distance ومقياس مسافة مانهاتن Manhattan distance . حيث تم في تجارب هذه الدراسة استخدام مقياس المسافة مانهاتن الموزونة كطريقة لتصنيف المستخدمين نظرا لأنه قدم افضل نتائج في [5] بعد مقارنته بمقاييس المسافة الاخرى.

تعتمد أغلب نظم المصادقة البيومترية المستمرة على ما يسمى بالعتبة ومستوى الثقة وقيمة القفل للتمييز بين المدخلات المقبولة والمرفوضة للمستخدمين، تمثل العتبة قيمة معينة تستقى من بيانات التدريب للمستخدمين. وهي النقطة التي يصبح فيها من المؤكد الى حد كبير إنَّ العينة البيومترية تتطابق مع قالب المقارنة. ويوجد نوعان للعتبة هما العتبة العامة وهي عبارة عن عتبة واحدة لجميع المستخدمين، والعتبة الفردية وهي التي يتم ضبطها لتتناسب مع مستخدم معين. بينما يعبر مستوى الثقة عن قيمة تتغير بناء على نمط الكتابة للمستخدمين حيث تزداد الثقة في المستخدم في حال تشابه او اقتراب نمط طباعته من قالب المقارنة وتقل إذا ما حدث عكس ذلك. وتمثل قيمة القفل قيمة معينة، فإذا تساوت معها قيمة مستوى الثقة فإنَّ النظام يقوم برفض المستخدم وعندها عليه استخدام آلية المصادقة الثابتة للدخول مرة أخرى للنظام.

قد تم في تجارب هذه الدراسة استخدام العتبة الفردية حيث اثبتت الدراسات إنَّها تقدم نتائج أفضل من العتبة العامة [5]، وتم استخلاص قيمة هذه العتبة من بيانات مرحلة التدريب بالطريقة الموضحة في [14] . حيث أصبح لكل شخص مستهدف في التجربة عتبة خاصة بكل كلمة من الكلمات قيد الدراسة. وتم تحديد قيم مستوى الثقة بعلاقة عكسية مع مستوى الثقة من الصفر (0)

الذي يمثل أعلى درجة ثقة بالمستخدم حيث لا تقل قيمة مستوى الثقة عن صفر، إلى ثلاثة (3) التي تمثل قيمة القفل (درجة انعدام الثقة بالمستخدم). يوضح الشكل6 خوارزمية المصادقة المنفذة.

```
foreach user do
 {
   foreach word do
   {
       foreach two consecutive keys do
      {
        compute PP, RR, PR, RP ;
        if (D > T_distance)
             increase C by 1 ;
          else
             decrease C by 1;
        }
   }
     if (C < T_lockout)
       user continues access ;
     else
       log out user ;
}
```

شكل6: خوارزمية المصادقة المستمرة على أساس ديناميكية المفاتيح

بعد مرحلة التدريب (التسجيل في التطبيق) يمكن للمستخدم تسجيل الدخول للتطبيق بكتابة اسم المستخدم وكلمة المرور وعند هذه النقطة تكون قد تمت مرحلة المصادقة الثابتة على المستخدم ومنها ينتقل الى مرحلة المصادقة المستمرة التي يمكن ان يكون فيها المشارك يمثل المستخدم الحقيقي او يتقمص دور المنتحل بعد تزويده باسم المستخدم وكلمة المرور الخاصة بالمستخدم الحقيقي بحيث يطلب من المشارك كتابة نص بريد الكتروني على ان لا يقل عدد الكلمات قيد الدراسة المستخدمة فيه عن تسعة كلمات وذلك نظرا لأنه اثناء القيام بالتجارب المبدئية تبين ان هذا القدر من الكلمات كافي لاكتشاف المنتحل. بعد اجتياز المستخدم مرحلة المصادقة الثابتة يمنح التطبيق المستخدم اعلى مستوى من الثقة وذلك بتعين القيمة صفر كقيمة مستوى الثقة، وخلال مرحلة المصادقة المستمرة يقل او يزداد مستوى الثقة بناء على قرب او بعد نمط طباعة المستخدم للكلمات قيد الدراسة من قالب المقارنة كما هو مبين في الشكل7، واذا تساوى مستوى الثقة مع قيمة القفل يقوم التطبيق بالقفل على المستخدم وعندها عليه استخدام آلية المصادقة الثابتة للدخول مرة أخرى للتطبيق.

شكل7: يوضح واجهة مرحلة المصادقة المستمرة

3. وصف التجربة

تمت التجارب خلال فترة اربعة أشهر على مدار عدة ايام تفصل بينها فترات زمنية مختلفة ، ففي الاول تمت مرحلة التدريب (تسجيل المشاركين في التطبيق)، وفي اليوم الثاني تمت مرحلة المصادقة بعد مرور اسبوع من نهاية المرحلة السابقة حيث استخدم كل مشارك حسابه الذي تم انشائه في مرحلة التدريب فقط، وفي اليوم الثالث بعد مرور شهر من نهاية المرحلة السابقة تمت مرحلة المصادقة ايضا ومن ثم حاول كل مشارك انتحال هوية ثلاثة من المشاركين المصنفين لذات الفئة المصنف اليها، وفي اليوم الرابع بعد مرور شهرين من نهاية المرحلة السابقة تمت مرحلة المصادقة ايضا ومن ثم حاول كل مشارك انتحال هوية اربعة مشاركين اثنين من كل فئة من الفئتين الغير مصنف اليها.

النتائج و المناقشة

تم جمع نتائج التجربة في شكل مصفوفة ارباك أو تشويش confusion matrix لتحليلها، حيث تتكون مصفوفة الارباك من العناصر التالية:

الإيجابيات الحقيقية (TP) : عدد مرات قبول المستخدمين الحقيقين.
السلبيات الحقيقية (TN) : عدد مرات رفض المنتحلين.
الإيجابيات الخاطئة (FP) : عدد مرات قبول المنتحلين.
السلبيات الخاطئة (FN) : عدد مرات رفض المستخدمين الحقيقين .

بناءً على كل ادخال لكلمة من الكلمات قيد الدراسة في التجربة تم انشاء مصفوفة ارباك خاصة بالكلمات شائعة الاستخدام كما هو مبين بالجدول1، واخرى خاصة بالكلمات نادرة الاستخدام كما هو مبين بالجداول2. ومن ثم تم حساب معدل القبول الخاطئ FAR ومعدل الرفض الخاطئ لكل مصفوفة ومنهما تم إيجاد معدل الخطأ المتساوي EER رياضيا باستخدام المعادلة (1) :

$$EER = (FAR + FFR)/2 \qquad (1)$$

: يوضح مصفوفة الارباك لنتائج ادخال الكلمات قيد الدراسة شائعة الاستخدام

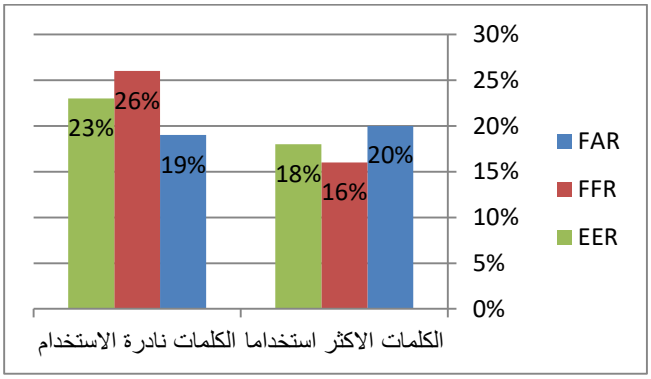
عدد الكلمات قيد الدراسة شائعة الاستخدام المكتوبة خلال التجربة ككل	عدد الكلمات شائعة الاستخدام المكتوبة من قبل المشاركين المتوقع انهم حقيقين	عدد الكلمات شائعة الاستخدام المكتوبة من قبل المشاركين المتوقع انهم منتحلين	
عدد الكلمات شائعة الاستخدام المكتوبة من قبل المشاركين الحقيقين بالفعل	TP (الجلسة الاولى) = 177 TP (الجلسة الثانية) = 212 TP (الجلسة الثالثة) = 212	FN (الجلسة الاولى) = 46 FN (الجلسة الثانية) = 44 FN (الجلسة الثالثة) = 27	718
عدد الكلمات شائعة الاستخدام المكتوبة من قبل المنتحلين بالفعل	FP (الجلسة الاولى) = 0 FP (الجلسة الثانية) = 155 FP (الجلسة الثالثة) = 140	TN (الجلسة الاولى) = 0 TN (الجلسة الثانية) = 458 TN (الجلسة الثالثة) = 689	1442
	896	1264	2158 = N

جدول2: يوضح مصفوفة الارباك لنتائج ادخال الكلمات قيد الدراسة نادرة الاستخدام

عدد الكلمات قيد الدراسة نادرة الاستخدام المكتوبة خلال التجربة ككل	عدد الكلمات نادرة الاستخدام المكتوبة من قبل المشاركين المتوقع انهم حقيقين	عدد الكلمات نادرة الاستخدام المكتوبة من قبل المشاركين المتوقع انهم منتحلين	
عدد الكلمات نادرة الاستخدام المكتوبة من قبل المشاركين الحقيقين بالفعل	TP (الجلسة الاولى) = 52 TP (الجلسة الثانية) = 48 TP (الجلسة الثالثة) = 62	FN (الجلسة الاولى) = 19 FN (الجلسة الثانية) = 20 FN (الجلسة الثالثة) = 17	218
عدد الكلمات نادرة الاستخدام المكتوبة من قبل المنتحلين بالفعل	FP (الجلسة الاولى) = 0 FP (الجلسة الثانية) = 31 FP (الجلسة الثالثة) = 23	TN (الجلسة الاولى) = 0 TN (الجلسة الثانية) = 106 TN (الجلسة الثالثة) = 121	281
	216	283	499 = N

اظهر تحليل نتائج التجربة انخفاض معدل EER لأداء نظام المصادقة قيد الدراسة بشكل عام، وهذا يدل على ان اداء النظام جيد مقارنة بالدراسات في ذات المجال التي استخدمت لغات اخرى.

وعن تجربة المصادقة باستخدام الكلمات نادرة الاستخدام نتج انخفاض طفيف في اداء النظام عند مقارنته مع اداء النظام في تجربة المصادقة باستخدام الكلمات شائعة الاستخدام كما هو موضح بالشكل8، واتضح ذلك في ارتفاع نسبة الرفض الخاطئ عند كتابة المشاركين لهذه الكلمات، حيث نتج عن استخدام الكلمات نادرة الاستخدام في المصادقة على المستخدمين معدل FAR بنسبة 19% ومعدل FRR بنسبة 26% ومعدل EER بنسبة 23%، في حين نتج عن استخدام الكلمات شائعة الاستخدام في المصادقة على المستخدمين معدل FAR بنسبة 20% ومعدل FRR بنسبة 16% ومعدل EER بنسبة 18%.



شكل8: يوضح الفرق في معدلات الاداء بين الكلمات شائعة استخدام و الكلمات نادرة الاستخدام

الخلاصة و التوصيات

أثبتت نتائج التجارب التي أجريت في هذه الورقة نجاح المصادقة على أساس ديناميكية مفاتيح اللغة العربية للنص الثابت في مصادقة المستخدمين مصادقة مستمرة خاصة في مصادقة المستخدمين الذين لديهم خبرة معقولة في الطباعة على لوحة المفاتيح. حيث كانت نسبة معدل الخطأ المتساوي EER الناتجة منخفضة. و أثبتت كذلك انه يمكن الاعتماد على ديناميكية المفاتيح لكلمات محددة (نص ثابت) في المصادقة على المستخدمين مصادقة مستمرة على ان تكون هذه الكلمات كثيرة الاستخدام في التطبيق او النظام الذي يستخدم هذا النوع من المصادقة، حيث ادى استخدام الكلمات نادرة الاستخدام في المصادقة الى انخفاض طفيف في اداء نظام المصادقة المبني على ديناميكية المفاتيح.

ونظراً لمحدودية هذه الدراسة من حيث عدد المستهدفين في التجارب التي أجريت وعدد الكلمات المدروسة المختارة فإننا نوصي بإجراء تجارب أكثر توسّعا بزيادة عدد المستهدفين وعدد الكلمات المدروسة أيضاً، مع محاولة عدم تقييد المستخدم بكلمات أو نصوص معينة. وكذلك نوصي باستخدام المصادقة المستمرة على أساس ديناميكية المفاتيح اللغة العربية في نظم المصادقة على النظم والتطبيقات العربية المحتاجة الى مستوى أمان إضافي لما لهذا النوع من المصادقة من دور فعال في تحسين تجربة المستخدم وكذلك صعب الاختراق وغير مكلف.

المراجع

[1]- Patrick Bours and Hafez Barghouthi, Continuous Authentication using Biometric Keystroke Dynamics, The Norwegian Information Security Conference (NISK) 2009.

[2]- Abdullah Alshehri, Frans Coenen, Danushka Bollegala, Iterative Keystroke Continuous Authentication: A Time Series Based Approach, Springer KI - Künstliche Intelligenz (2018) 32:231–243.

[3]- Dina El Menshawy, Hoda Mokhtar, and Osman Hegazy, A Keystroke Dynamics Based Approach for Continuous Authentication, Springer International Publishing Switzerland 2014.

[4]- Rohit A. Patil and Amar L. Renke, Keystroke Dynamics for User Authentication and Identification by using Typing Rhythm, International Journal of Computer Applications (0975 – 8887) Volume 144 – No.9, June 2016.

[5]- Fred Rundhaug, Keystroke dynamics Can attackers learn someone's typing characteristics, Master thesis in Information Security - Department of Computer Science and Media Technology - Gjøvik University College 2007.

[6]- Eesa Alsolami, An Examination of Keystroke Dynamics For Continuous User Authentication, PhD thesis - Information Security Institute - Science and Engineering Faculty - Queensland University of Technology 2012.

[7]- Romain Giot, Mohamad El-Abed and Christophe Rosenberger, Fast computation of the performance evaluation of biometric systems: application to multibiometric, Future Generation Computer Systems (FGCS).

[8]- Tiago Oliveira, Improving Web Authentication with Keystroke Dynamics , Masters thesis in Computer Engineering -IT department - Do Minho University 2014.

[9]- Pin Shen Teh, Andrew Jin Teoh and Shigang Yue, A Survey of Keystroke Dynamics Biometrics, The Scientific World Journal Volume 2013, Article ID 408280, 24 pages.

[10]- K. G. Srinivasa and Soumya Gosukonda, Continuous multimodal user authentication: coupling hard and soft biometrics with support vector machines to attenuate noise, CSIT 2014.

[11]- Issa Traoré and Ahmed Awad , Continuous Authentication Using Biometrics: Data, Models, and Metrics: Data, Models, and Metrics, Published in the United States of America by Information Science Reference (an imprint of IGI Global) 2012.

[12]- Jonathan Ness, Presentation Attack and Detection in Keystroke Dynamics, Master thesis in Information Security - Department of Information Security and Communication Technology - Norwegian University of Science and Technology 2017.

[13]- Pin Teh, Andrew Jin Teoh and Shigang Yue , A Survey of Keystroke Dynamics Biometrics, Hindawi Publishing Corporation - The Scientific World Journal 2013.

[14]- Jyoti Malik and Dhiraj Girdhar, Reference Threshold Calculation for Biometric Authentication, I.J. Image, Graphics and Signal Processing, 2014, 2, 46-53 Published Online January 2014 in MECS.