مجلة العلوم البحثة والتطبيقية
Journal of Pure & Applied Sciences
www.Suj.sebhau.edu.ly ISSN 2521-9200
Received 03/02/2019 Revised 19/04/2019 Published online 01/05/2019

خوارزمية المصادقة المستمرة على أساس ديناميكية المفاتيح
(تطبيق على الكلمات العربية الاكثر استخداما في رسائل البريد الالكتروني e-mail)

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

الملخص تعتمد أغلب أنظمة الحاسوب على المصادقة الثابتة للمستخدم وهذا لا يضمن ان من يستخدم النظام هو ذاته من لحظة تسجيل الدخول الي لحظة تسجيل الخروج ، ولهذا نحن بحاجة إلى وجود نظام مصادقة يمكنه التحقق من ما إذا كان المستخدم قد تغير بعد إجراء تسجيل الدخول أو لا، ولهذا ظهرت المصادقة المستمرة بمختلف أساليبها لسد هذه الفجوة. و ديناميكية المفاتيح تعتبر احد اساليب المصادقة المستمرة سهلة التطبيق من عدة جوانب، لهذا تهدف هذه الورقة لدراسة مدى فاعلية تطبيق أحد خوارزميات المصادقة المستمرة Continuous Authentication للمستخدم على أساس ديناميكية مفاتيح اللغة العربية Keystroke Dynamics في تطور انظمة الامن في المستقبل، تم تطبيق الخوارزمية في هذه الدراسة على الكلمات العربية الأكثر استخداما في رسائل البريد الالكتروني e-mail، 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 المسافة الاقليدية. وقد أظهرت النتائج أنَّه من الممكن مصادقة المستخدمين مصادقة مستمرة استناداً إلى ديناميكية مفاتيح اللغة العربية.

الكلمات المفتاحية: أمن الحواسيب، المصادقة الثابتة، المصادقة المستمرة، ديناميكية المفاتيح، مصادقة المستخدم.

continuous authentication algorithms based on Keystroke Dynamics (Applied to the most frequently used Arabic words in e-mail messages)

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

Abstract Most computer systems rely on the static user authentication which does not guarantee that whoever uses the system is the same one from the moment of login to the moment of logout, so, we need to have an authentication system that can verify whether the user has been changed or not, after the login is made. For this reason, the continuous authentication of various methods has been emerged to bridge this gap. The dynamic key of continuous authentication is one of these methods that can be easily applied in many aspects. The purpose of this paper is to examine the effectiveness of applying one of the continuous authentication algorithms to the user based on the dynamic of Arabic Language Keystroke for the development of security systems in the future. In this study, the algorithm has been applied to the most frequently used Arabic words in e-mail، where four of the timing characteristics were used to extract the features of the typing style of users on the keyboard. To classify users' data, a measure of distance from the statistical approach, which is the Euclidean distance measure, was used. The results have shown that it is possible to authenticate users using continuous authentication based on the dynamics of the Arabic Language keys.

Keywords: Computer Security, Static Authentication, Continuous Authentication, Keystroke Dynamics, User Authenticate.

المقدمة

ازداد اعتماد البشر في العقود الاخيرة على الحاسوب في جميع انشطتهم الحياتية، ويعتبر امن الحاسوب جزء لا يتجزأ من اي نشاط حاسوبي، الا أن ضمان الأمن لا يزال يمثل مشكلة صعبة، وخاصة عند إجراء المعاملات التي يجب ان يكون فيها المستخدم متصل بالأنترنت online ، ومن الحلول الرئيسة للقضاء على التهديدات الأمنية هي المصادقة والتحكم في الوصول. تعمل المصادقة على التحقق من هوية المستخدم، بينما يقرر نظام التحكم في الوصول من يسمح له بالوصول إلى موارد النظام أو خدماته ويحدد الامتيازات [1] . يتم عادة تنفيذ مصادقة المستخدم بشكل ثابت عند لحظة دخوله للنظام، 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 [2]، وتوفير المزيد من الأمن المستمر ومكافحة

التهديد اثناء استخدام النظام، كما أدت الحاجة المتزايدة لتحسين نظم الأمن إلى مزيد من البحوث في تطبيق القياسات الحيوية (biometrics) داخل نظم المصادقة. القياسات الحيوية هي قياسات تعتمد على الخصائص الشخصية التي تميز بشكل فريد كل مستخدم عن الآخر مثل بصمات الأصابع والصوت [1]، وتعتبر ديناميكية المفاتيح أحد 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.

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 [1] 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 [3] تسعى لتحسين المصادقة على الانترنت ببناء نظام مصادقة ثابتة قائم على ديناميكية المفاتيح من الصفر على شكل تطبيق انترنت تفاعلي باستخدام استراتيجية النشر الهجين. وتهدف دراسة أخرى [4] إلى الإجابة عن السؤال "هل يمكن لمنتحل أن يتعلم خصائص الكتابة لشخص ما؟" فتم 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 Authentication

مصادقة المستخدم هي عملية التحقق مما إذا كانت هوية المستخدم حقيقية قبل منحه حق الوصول إلى الموارد أو الخدمات في بيئة آمنة [5]، فقد حددت الأبحاث الأمنية أنه من أجل تحديد هوية المستخدم بشكل قاطع، يفضل استخدام اثنين على الأقل من عوامل المصادقة، والافضل استخدام العوامل الثلاثة معا [6] وهذه العوامل متمثلة في الاتي:

1. **القائمة على المعرفة**

هذا النوع من العوامل يعتمد على شيء يعرفه فقط المستخدم الشرعي للهوية المزعومة، وهو من الطرق الأكثر شيوعاً للمصادقة على الأنظمة ويمثل كذلك شيئا لا يعرفه إلا المستخدم ككلمة المرور أو الرمز السري الذي من شأنه التحقق من هويته [7].

2. **القائمة على الاشياء المملوكة**

هذا النوع من العوامل يعتمد على عنصر مادي يجب أن يمتلكه فقط المستخدم الشرعي للهوية المزعومة، وعادة ما يكون هذا العنصر في شكل بطاقات عضوية او بطاقات ائتمان.

3. **القائمة على القياسات الحيوية**

هذا النوع من العوامل يعتمد على القياسات الحيوية التي تشير إلى بعض الخصائص الفسيولوجية أو السلوكية التي ترتبط بشكل فريد بشخص معين، وتعدّ هذه الخصائص مميزة للغاية ويمكن استخدامها للتمييز بين الأفراد المختلفين [8]. ومن خلال هذا النوع من المصادقة يتم التعرف على المستخدمين من خلال من هم بدلا من ما يعرفون أو يملكون [5].

القياسات الحيوية (البيومترية) Biometrics

يتمتع الناس بخصائص شخصية تحددهم بشكل فريد مثل توقيع اليد وبصمة الأصبع والصوت، وتعرف هذه الخصائص الفريدة باسم القياسات الحيوية وهي تقنية تسمح بالتعرف على الافراد من خلال تحليل الخصائص الفسيولوجية أو السلوكية الخاصة بكل فرد، وتوجد فئتان لتقنيات القياسات الحيوية وهي:

1. **البيولوجية**

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

2. **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 [9] :

- **معدل القبول الخاطئ** (FAR)

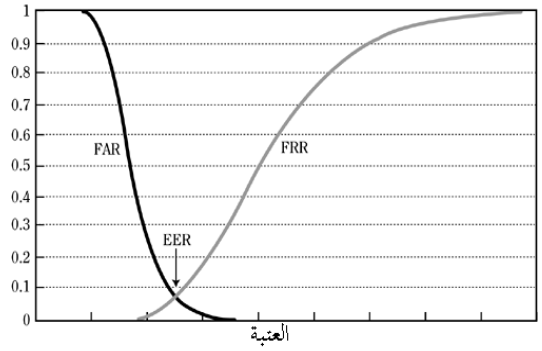
يشير FAR إلى النسبة المئوية بين المستخدمين غير المصرح لهم الذين تم قبولهم خطأ مقابل إجمالي عدد المنتحلين الذين يحاولون الوصول إلى النظام [10]، ويدل FAR المنخفض على قبول عدد منتحلين أقل.

- **معدل الرفض الخاطئ** (FRR)

يشير FRR إلى النسبة المئوية بين المستخدمين الحقيقيين الذين تم رفضهم خطأ مقابل إجمالي عدد المستخدمين الحقيقيين الذين يصلون إلى النظام [10]، 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 بالشكل رقم (1). ويدل EER المنخفض على ارتفاع دقة نظام المصادقة البيومترية.



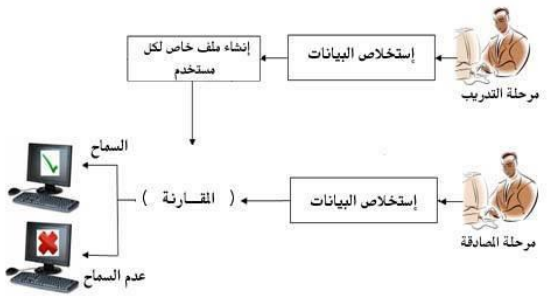
شكل رقم (1): يوضح مقاييس اداء النظم البيومترية FAR و FRR و EER

المصادقة الثابتة و المصادقة المستمرة

المصادقة الثابتة هي آلية تحقق من هوية المستخدم عند نقطة الدخول فقط للجلسة أي لحظة تسجيل الدخول [11]. في حين تشير المصادقة المستمرة الى آلية تحقق من هوية الفرد بشكل متكرر طوال مدة الجلسة [12] (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 أنّه ضعف أمني خطير في أنظمة الأمان العالي [11] ، 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 [7] .

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 شخصيًّا [10]، يبين الشكل رقم (2) آلية عمل ديناميكية المفاتيح.



الشكل رقم (2): آلية عمل ديناميكية المفاتيح كأسلوب مصادقة على المستخدم

تمَّ في العديد من الدراسات البحثية استخدام ديناميكية المفاتيح كآلية للمصادقة الثابتة تدعم المصادقة باستخدام اسم المستخدم وكلمة المرور من خلال رصد نمط كتابة المستخدم لهما أثناء لحظة تسجيل الدخول وعندها يتم مقارنته بالقالب المخزن مسبقا لذات المستخدم مثل [13]. وكذلك استخدمت ديناميكية المفاتيح كآلية للمصادقة المستمرة اما عن طريق استخدام النص الثابت وفيه يتم منح المستخدم نصاً محدداً مسبقًا (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 مثل [1]، أو عن طريق استخدام 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 مثل [14].

طريقة البحث

لتنفيذ الخوارزمية تم إجراء عدد من التجارب حيث كان حجم العينة متمثلًا في 12 شخصاً من الناطقين باللغة العربية ولديهم اختلاف في مهارات الكتابة على لوحة المفاتيح. تم تقديم عينات الطباعة باللغة العربية على جهاز واحد وذلك من خلال تطبيق انترنت تفاعلي باستخدام استراتيجية النشر الهجين الذي تم تصميمه لهذا الغرض، 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 أكثر عشر كلمات عربية استخداما في رسائل البريد الالكتروني e-mail وهي (مرحبا ،السلام عليكم ،تحية طيبة ،شكرا ،أمَّا 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.

يُطلب في مرحلة التدريب من الاشخاص المستهدفين التسجيل في النظام عن طريق كتابة اسم مستخدم وكلمة مرور من اختيارهم ومن ثم كتابة كل كلمة من الكلمات المدروسة عشرة مرات بطريقة طبيعية. استخدمت في هذه الدراسة ميزات ديناميكية المفاتيح الزمنية المستخدمة في [1] 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.

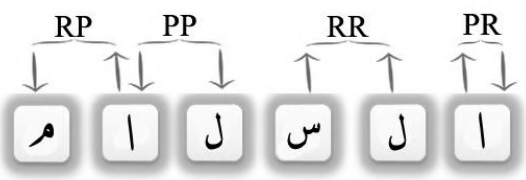
PR (Press-Release) : هي الفترة الزمنية بين الضغط على وافلات مفتاح واحد.

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 الشكل رقم (3) مثال لهذه الميزات عندما يدخل المستخدم كلمة "السلام".

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



الشكل رقم (3): 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 كتابته بطريق خطأ، 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 [10]، 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 الاقليدية كطريقة لتصنيف المستخدمين نظرا لبساطته وشيوع استخدامه في هذا المجال.

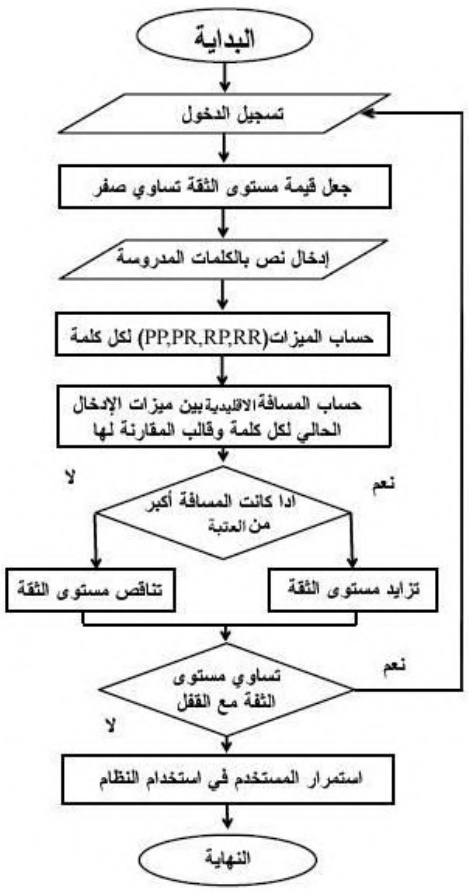
تعتمد أغلب نظم المصادقة البيومترية المستمرة على ما يسمى بالعتبة ومستوى الثقة وقيمة القفل للتمييز بين المدخلات المقبولة والمرفوضة للمستخدمين، تمثل العتبة قيمة معينة تستقى من بيانات التدريب للمستخدمين. وهي النقطة التي يصبح فيها من المؤكد الى حد كبير إنَّ العينة البيومترية تتطابق مع قالب المقارنة. ويوجد 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 فإنّ 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 إنّها تقدم نتائج أفضل من العتبة العامة، [4] وتم استخلاص قيمة هذه العتبة من بيانات مرحلة التدريب بالطريقة الموضحة في [15] . حيث أصبح لكل شخص مستهدف في التجربة عتبة خاصة بكل كلمة من الكلمات المدروسة .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 الشكل رقم (4) خوارزمية المصادقة المنفذة.

3. وصف التجربة

تمت التجارب خلال فترة ثلاثة أشهر بمعدل يوم في كل شهر، ففي اليوم الاول تم جمع بيانات مرحلة التدريب (التسجيل في التطبيق) من المستهدفين في التجربة، ثم طُلب من كل مستخدم الدخول للتطبيق باستخدام حسابه الخاص وإرسال رسالة بريد الكتروني تحتوي على أكبر قدر ممكن من الكلمات المدروسة، وفي اليوم الثاني (بعد مرور شهر على اليوم الاول للتجربة) طُلب من كل مستخدم استخدام التطبيق باستخدام حسابه الخاص ثم طُلب منهم محاولة انتحال هوية ثلاثة مستخدمين آخرين، وفي اليوم الثالث (بعد مرور شهر على اليوم الثاني للتجربة) طُلب من كل مستخدم استخدام التطبيق باستخدام حسابه الخاص ثمَّ طُلب منهم أيضا محاولة انتحال هوية ثلاثة مستخدمين آخرين غير الذين حاولوا انتحال هويتهم في اليوم السابق.



الشكل رقم (4): خوارزمية المصادقة المستمرة على أساس ديناميكية المفاتيح

النتائج و المناقشة

نتج من اليوم الأوّل للتجربة إدخال عدد (119) للكلمات المدروسة من قبل المستخدمين الحقيقين، كان منها عدد (39) إدخال خاطئ (نمط كتابة الكلمة المدخلة بعيد عن قالب المقارنة المخزن في قاعدة البيانات للمستخدم)، ونتج من اليوم الثاني عدد (112) إدخال للكلمات المدروسة من قبل المستخدمين الحقيقين كان منها عدد (24) إدخال خاطئ، وعدد (172) إدخال للكلمات المدروسة من قبل المنتحلين كان منها عدد (53) إدخال صحيح، وعن اليوم الثالث عدد (120) إدخال للكلمات المدروسة من قبل المستخدمين الحقيقين كان منها عدد (18) إدخال خاطئ، وعدد (162) إدخال للكلمات المدروسة من قبل المنتحلين كان منها عدد (46) إدخال صحيح.

تم ملاحظة تطور اداء المشاركين من حيث استقرار نمط كتابتهم وقربه من قالب المقارنة وكذلك انخفاض عدد ادخالاتهم الخاطئة كمستخدمين حقيقين في اليوم الثاني والثالث للتجربة. ومن المرجح أنَّ سبب هذا التطور هو أنهم اعتادوا الطباعة على لوحة مفاتيح جهاز الكمبيوتر المستخدم في التجربة.

تم جمع نتائج التجربة في شكل مصفوفة ارباك أو تشويش confusion matrix لتحليلها كما هو موضح في الشكل رقم (5) بناء على كل ادخال لكلمة من الكلمات المدروسة بالشكل التالي :

الإيجابيات الحقيقية (TP) : الإدخالات المقبولة من قبل المستخدمين الحقيقين .

السلبيات الحقيقية.(TN): الإدخالات المرفوضة من قبل المنتحلين.

الإيجابيات الخاطئة (FP): الإدخالات المقبولة من قبل المنتحلين .

السلبيات الخاطئة (FN) : الإدخالات المرفوضة من قبل المستخدمين الحقيقين .

N: عدد الكلمات المدروسة المكتوبة خلال التجربة ككل.

	عدد الكلمات المدروسة المكتوبة من المشاركين المتوقع انهم حقيقين	عدد الكلمات المدروسة المكتوبة من المشاركين المتوقع انهم منتحلين	
عدد الكلمات المدروسة المكتوبة من المشاركين الحقيقين بالفعل	TP = 270	FN = 81	351
عدد الكلمات المدروسة المكتوبة من المنتحلين بالفعل	FN = 97	TN = 237	334
	367	318	N = 685

الشكل رقم (5): مصفوفة الارباك لنتائج التجربة

وتم الحصول على معدل FAR بنسبة 0.23% ومعدل FFR بنسبة 0.29% ومنهما تم إيجاد معدل EER بنسبة 0.26% رياضيا باستخدام المعادلة التالية :

$$ER = (FAR + FFR)/2$$

تعتبر نسبة EER المتحصل عليها من التجربة منخفضة و مقبولة مقارنة بالدراسات المشابهة في ذات المجال .

الخلاصة و التوصيات

من خلال التجارب التي أجريت في تنفيذ خوارزمية المصادقة المستمرة أثبتت النتائج نجاح المصادقة على أساس ديناميكية مفاتيح اللغة العربية 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.

بهذا تعتبر ديناميكية المفاتيح طريقة واعدة وغير مكلفة في مجال أنظمة المصادقة المستمرة لأنها لا تحتاج الى اي أجهزة إضافية وكذلك حائزة على رضا المستخدم نظرا لأنها لا تحتاج إلى أيِّ مجهود إضافي منه، فكلُّ ما يجب عليه هو التفاعل بشكل طبيعيٍ مع النظام المستخدم .

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 أو تقيده بعدم ارتكاب أخطاء أثناء الطباعة أو جهاز كمبيوتر محدد. ويفضل استخدام أجهزة الكمبيوتر الخاصة بالمشاركين.

المراجع

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

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

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

[4]- 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.

[5]- Patrick Bours and Soumik Mondal, Recent Advances in User Authentication Using Keystroke Dynamics Biometrics, Science Gate Publishing 2015.

coupling hard and soft biometrics with support vector machines to attenuate noise, CSIT 2014.

[12]- 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.

[13] Yu Zhong, Yunbin Deng and Anil Jain, Keystroke Dynamics for User Authentication, IEEE 2012 .

[14] Paulo Pinto, Bernardo Patrao and Henrique Santos, Free Typed Text Using Keystroke Dynamics for Continuous Authentication, Conference on Communications and Multimedia Security (CMS), Aveiro, Portugal 2014.

[15] 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.

[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]- 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.

[8]- 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.

[9]- 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).

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

[11]- K. G. Srinivasa and Soumya Gosukonda, Continuous multimodal user authentication: