مجلة العلوم البحتة والتطبيقية
Journal of Pure & Applied Sciences
www.Suj.sebhau.edu.ly ISSN 2521-9200
Received 13/03/2020 Revised 11/08/2020 Published online 05/10/2020

تأثير مستوى تعقيد كلمة المرور على إنتاج نموذج موثوق لخصائص ديناميكية المفاتيح

*سلوى عبدالنبي إبراهيم على[1] و خميس مسعود سالم احمد[2]
[1]قسم الشبكات والاتصالات–كلية تقنية المعلومات–جامعة سبها، ليبيا
[2]قسم علوم الحاسب–كلية تقنية المعلومات–جامعة سبها، ليبيا
*للمراسلة: sal.ali1@sebhau.edu.ly

الملخص تعتبر المصادقة الالكترونية إحدى أهم المشاكل التي تواجه آلية الوصول إلي مصادر المعلومات، ففي عصر يعتمد بشكل كامل على الحسابات الافتراضية ، لم يعد تعقيد الكلمة السرية مجدياً لحمايتها من الاختراق. وبالتالي جاءت الحاجة لابتكار تقنيات جديدة لتعزيز مستوى الأمن الذي توفره كلمات المرور لحماية بيانات المستخدم. تعتبر ديناميكية الضغط على لوحة المفاتيح (keystroke dynamics) أحد التقنيات للتعرف على هوية المستخدمين اعتمادا على سلوكياتهم أثناء الطباعة على لوحة المفاتيح . تهدف هذه الدراسة الي التعرف على الطرق المختلفة للمصادقة الإلكترونية أو التحقق من الهوية كما تسلط الضوء على استخدام ديناميكية الضغط على لوحة المفاتيح كأداة قوية من الممكن توظيفها الى جانب كلمة المرور للتحقق من هوية المستخدم. تقدم هذه الورقة دراســـة نظرية وتحليلية لاستخدام ديناميكيـــة لوحة المفاتيـــح في إنتاج نمـــوذج لخصائص المستخدم السلوكيـــة باختلاف نوع كلمة المرور. تم تطوير تطبيق برمجي بلغة الجافا لإجراء تجربة لمحاكاة مرحلة التسجيل لتجميع البيانات الزمنية للمستخدمين عند تفاعلهم مع لوحة المفاتيح لإدخال ثلاث كلمات مرور بدرجات تعقيد متفاوتة ومن ثم استخلاص الخصائص السلوكية وتطبيق خوارزمية التصنيف المعتمدة على المعايير الاحصائية. أظهرت الدراسة أن استخدام كلمات المرور المتوسطة التعقيد والمعقدة تعطي نتائج أفضل من كلمة المرور البسيطة، وأكدت أيضاً ما توصلت اليه الدراسات السابقة من نتائج. كما تبين أن استخدام الخصائص المتصلة (الزمن الكلي للكتابة) المرتبط بكلمة المرور المعقدة هو الافضل لتمييز المستخدمين عن بعضهم مع الاخذ بالاعتبار سلوكياتهم عند كتابة الحروف الكبيرة والأرقام.

الكلمات المفتاحية: القياسات الحيوية، ديناميكية الضغط، التحقق من هوية، الخصائص، السلوكية، خوارزمية التصنيف، كلمة المرور.

The Impact of Password complexity level on Building a Reliable Model of Keystroke Features

*Salwa A.I. Ali[a], Khamiss M. S. Ahmed[b]
[a] Department of Network and communication Faculty of Information Technology Sebha University,Libya
[b] Department of Computer Science Faculty of Information Technology Sebha University,Libya
*Corresponding author: sal.ali1@sebhau.edu.ly

Abstract Electronic authentication is considered to be one of the most important problems in the field of accessing information sources. In an era that relies entirely on virtual accounts, the complexity of the password is no longer effective to protect it from penetration. This necessitates the use of new technologies to enhance the level of security that passwords provide to protect users' data. Keystroke dynamics is a technique for identifying users based on their behavior on the keyboard. This study aims to identify the various methods of authentication and highlights the use of keystroke dynamics as a powerful tool that can be used alongside the password to verify the identity of the user. This paper provides a theoretical and analytical study of the use of the keystroke dynamics in producing a model for the behavioral user characteristics according to the type of password. A software application was developed by Java language to conduct an experiment to collect time data for users when they interact with the keyboard to enter three passwords of different complexity levels and then extract behavioral characteristics and the applying statistical classification algorithm. The study showed that the use of medium-complex and complex passwords give better results than the simple password, and also confirmed the results of previous studies. It was also found that the use of aggregated features (total typing time) associated with a complex password is the best to distinguish users from one another while taking into account their behavior when writing large letters and numbers.

Keywords: keystroke dynamics, familiar password, features, biometric template, enrolment, access control.

المقدمة

تلعب المعلومات في العصر الحالي المعروف بعصر المعلومات دوراً حيوياً في نجاح أي منظمة بغض النظر عن نوعها حكومي أو خاص.، أمن تلك المعلومات أمر ضروري للمنظمات التي تهتم بحماية ممتلكاتها وخاصةً أصولها الفكرية من الوقوع في أيدي قراصنة الشبكات، وبهذا ازدادت الحاجة إلى التحقق من الأشخاص سواءً من داخل المؤسسة أو خارجها لضمان عدم تغييرهم لها أو التلاعب بها وحذفها. لذلك فإن ادارة قواعد البيانات في حاجة إلى وجود آلية للتحقق من هوية الشخص قبل السماح له بالوصول الى المعلومات المخزنة بها[1].

من أهم وأشهر الطرق المستخدمة في التحقق من الهوية كلمات المرور (passwords)، وبالرغم من مرونة استخدام هذه الطريقة إلا إنها أصبحت غير مرضيه من حيث التوازن بين الجانب الأمني وسهولة الاستخدام، الأمر الذي يجعلها سهلة الكسر من قبل المخترقين[15].

القياسات الحيوية (Biometrics) هي أحد أقوى الطرق المستخدمة في تحقيق المصادقة الالكترونية من الناحية الأمنية لاعتمادها علي الخصائص الوراثية أو الحيوية للأشخاص، حيث تصنف القياسات الحيوية إلى نوعين: فيزيائيـــة وسلوكيـــة . تمثل الخصائص الفيزيائية ميزات المستخدم الوراثية مثل بصمة الأصبع (Finger Print) ، بينما تضم الخصائص السلوكية الطريقة التي تميز المستخدم عن غيره من الناحية السلوكية مثل نبرة الصوت وديناميكية الضغط علي لوحة المفاتيح[12].

إيقاع الطباعة على لوحة المفاتيح (Keystroke dynamics) أحد الأنواع التي تندرج تحت القياسات السلوكيـــــــة للمستخـــــــــدمين ، والتي تعتـــــــــــــــمد على التعرف على المستخدم عن طريق سلوكـــــــــــه عند التعامل مع لوحة المفاتيح، حيث يتم ذلك بتحديد مجموعة الخصائص ذات الطابع التي تمثل المستخدم أثناء استخدامه للوحة المفاتيح مثل زمن ضغط المفتاح (dwell time)، زمن الطيران(Flight Time)، أو الانتقال بين المفاتيح بالإضافة إلى سرعة الطباعة نظراً لاعتماد هذه الطريقة بشكل رئيسي على البرمجيات فإنه بالإمكان الاستفادة من مميزاتها واستخدامها كعامل إضافي إلى جانب كلمات المرور للتحقق من هوية المستخدم[18].

تعدد الخصائص الزمنية المرتبطة باستخدام الـــ Keystroke dynamics يجعل اختيار الأفضل من بينها لتمثيل المستخدم معقد نسبياً، بالإضافة إلى تأثير الحالة النفسية والصحية للمستخدم على سلوكه مما يجعل خصائص المستخدم السلوكية عرضه لمجموعة من التغيرات والتي من الممكن ان تؤثر سلباً على مستوى تفّرده عن غيره من المستخدمين ، الأمر الذي يجعل أيضاً عملية الحصول على نموذج ثابت لخصائص المستخدم السلوكية عند طباعة كلمة المرور يختلف باختلاف نوع كلمة المرور المستخدمة. [26].

تتركز أهميـــــة هذه الدراسة في التعريف بنوع كلمة المرور التي تجعل استخدام ايقاع طباعة المستخدم على لوحة المفاتيح في المصادقة الالكترونيـــــة أكثر كفاءة وفعاليـــــة وبالتالي الموازنة بين كلٍ من الأمنيـــــة وسهـــــولة الاستخدام.

أمن المعلومـــــات

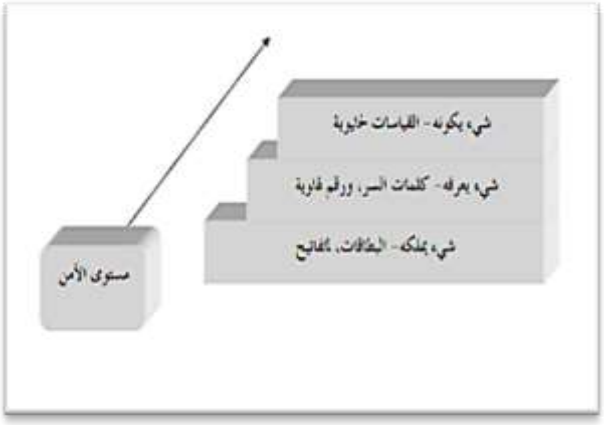
إنّ التقدم التكنولوجي الكبير، وتطوّر وسائل التواصل والاتصال المتنوعة، أدى إلى إحداث مشاكل أمنية متمثلة في تسرّب البيانات ووصولها للأشخاص الغير مخولين بالوصول إليها، وبالتّالي أصبحت الحاجة ملحّة للحفاظ على أمن المعلومات. ويعّرف أمن المعلومات، أنه مجموعة الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية[1]. وتتألف عملية أمن المعلومات من أربعة عناصر مهمة [10].

- **السرية أو الموثوقية Confidentiality**: وتعني التأكد من ان المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
- **التكاملية وسلامة المحتوى Integrity:** التأكد من ان محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في اية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.
- **استمرارية توفر المعلومات أو الخدمة Availability**: التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وان مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.
- **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به Non-repudiation:** ويقصد به ضمان عدم انكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها انكار انه هو الذي قام بهذا التصرف ، بحيث تتوفر قدرة اثبات ان تصرفا ما قد تم من شخص ما في وقت معين.

التحقق من الهوية أو المصادقة (Authentication) الالكترونيـــــة

المصادقة هي عملية التحقق من صحة ادعاء ما؛ وبمعنى اخر، تحديد ما اذا كان الشخص الذي يحاول الدخول للنظام هو نفسه صاحب الحساب أو شخص آخر (مهاجم) [17]. يوفر التحقق من الهوية أجابه لسؤالين: الأول : من هو المستخدم؟ والثاني : هل المستخدم هو الشخص الذي يجب أن يتعامل مع المعلومات و بدقة أكثر؟، وكما هو موضح في الشكل (1) ، فإن أدوات التحقق من الهوية تُصنف الى ثلاثة أنواع أساسية[26]:

- شيء يملكه المستخدم مثل visa card.
- شيء يعرفه المستخدم مثل passwords.
- شيء يُكوّن المستخدم أو يمثله كخصائصه الحيـــوية Biometrics.



شكل 1: تصنيف طرق التحقق من الهوية [25]

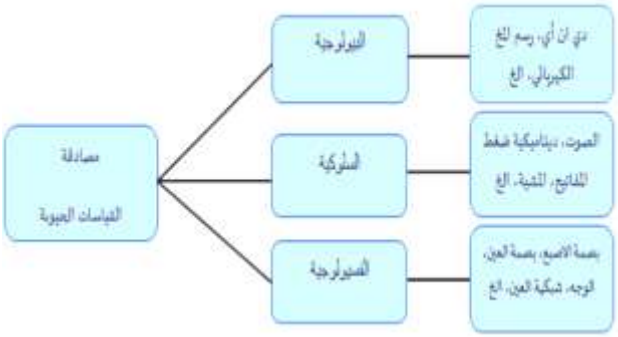
كلمـــــات المرور Passwords

هي أحد أشهر الطرق المستخدمة في المصادقة الالكترونية ، والتي تعتمد بشكل أساسي على ادخال كلمة المرور الصحيحة للدخول للنظام ، وبالتالي ينبغي أن تكون هذه الكلمة سرية وغير معروفة للأشخاص الغير مخولين بالوصول للنظام . كلمة المرور يجب أن تكون قوية لتوفير الحماية من الذين يحاولون اختراقها[1] .

لم يشهد استخدام كلمات المرور مشاكل عديدة في بداية توظيفها بسبب قلة المستخدمين ، ولكن مع ازدياد عدد المستخدمين ظهرت العديد من المشاكل المتعلقة بسهولة تخمينها نظراً لاعتماد المستخدمين كلمات مرور بسيطة سهلة التذكر للمستخدمين كتواريخ ميلادهم أو أسماء أصدقائهم أو أرقام هواتفهم.... إلخ . وبالتالي وعلى الرغم من سهولة توظيف كلمات المرور بالنسبة لمديري الانظمة ، إلا أنها تعانـــي من بعض نقاط الضعف والمتمثلة في عدم الموازنة بين مستوى الامنيـــة في اختيار كلمة مرور معقدة وسهـــولة الاستخدام [9].

القيـــاسات الحيوية (Biometrics)

القياسات الحيوية تعتبر من أفضل الطرق المستخدمة في المصادقة الالكترونيـــة؛ لأنها تعطي درجة عالية من الأمان مقارنة بالأساليب الأخرى ،حيث لا يمكن نسيانها أو سرقتها أو فقدها كما في كلمات السر والبطاقات والمفاتيح، لذا هناك اتجاه الآن في مجال أمن الحاسبات والمعلومات باستبدال كلمات السر والبطاقات الذكية بالقياسات الحيوية واستخدامها لتحديد هوية الشخص والتعرف عليه، والسماح له بالوصول جسدياً أو منطقياً. إلى مبنى، أو حاسب آلي، أو قاعدة بيانات[2].



شكل 2: تصنيف انظمة Biometric

يستخدم المعيار الثنائي للتحقق من الهوية (Two factor authentication) لإضافة المزيد من الأمان لعملية المصادقة عن طريق الربط بين ميزات أكثر من أداة نظراً لاختلاف مستوى التمييز الذي توفره أكثر من أداة واحدة، وبالتالي فأن استخدام القياسات الحيوية كمعيار إضافي للتحقق من الهوية من شأنه تعزيز مستوى الأمان للأنظمة [12].

وفقاً للتطبيق المطلوب، يمكن استخدام نظم القياسات الحيوية إما لإثبات الهوية (Verification) أو تحديد الهوية (Identification). ويتحقق النظام في حالة إثبات الهوية (Authentication) من أن هوية الشخص هي بالفعل كما يدّعيها بناءً على البيانات المسجلة عنه مسبقاً (one –to-one) ، وفي حالة تحديد الهوية فإن نظام القياسات الحيوية يحدد الشخص من بين جميع الأشخاص المسجلين في قاعدة البيانات أي أن النظام يعمل على تحديد من يكون هذا الشخص(one-to-many).

تصنيـــف القيـــاســـات الحيوية Biometrics classification

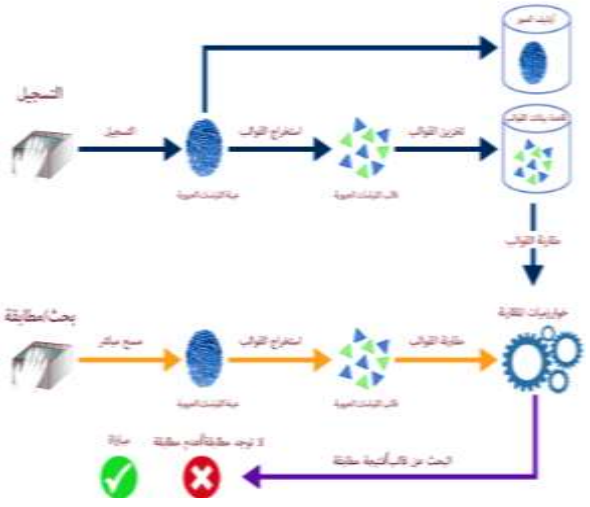
تقسم القياسات الحيوية إلى فئتين: الخصائص الجسدية (المادية/الفسيولوجية) Physical characteristics، والخصائص السلوكية Behavioral characteristics ،

ويطلق على الفئة الأولى اسم الثابتة (Static) حيث تعتمد على استخلاص البيانات من القياسات التشريحية للشخص. أما الفئة الثانية فيطلق عليها القياسات الديناميكية (Dynamics) وهي أقل ثباتاً من الأولى، وتتغير مع الضغط أو الضعف، كما أنها أقل أماناً. ولكنها تمتلك ميزة عن الفئة الأولى حيث من الممكن أن تكون غير واضحة للشخص، أي يمكن تحديد هويته دون أن يدري أنه خضع لهذه العملية– وهي أكثر قبولاً من قبل الأشخاص لأنها أقل تطفلاً [20].

ينبغي أن تكون السمات الجسدية والسلوكية المستخدمة من أجل التعرف فريدة، أي أنها تكون موجودة في شخص واحد فقط وألا تظهر في شخصين على مستوى العالم، ودائمة الزمن أو لا يمكن تغييرها، وقابلة للقياس، أي تكون قابلة للقياس باتساق باستخدام الأدوات التقنية، كما يجب أن تكون المعلومات التي تم قياسها قابلة للتخزين على نحو فعال، وقابلة للمقارنة في قاعدة البيانات المرجعية الحيوية بحيث يمكن باستخدامها تحديد الفرد والتأكد منه [3].

تقنيـــات القياســـــات الحيـــــوية

تختلف تقنيـــات القياسات الحيوية في تعقيدها، وقدراتها وأدائها إلا أنها تتشارك في العديد من العناصر، فهي نظم صممت أساساً للتعرف على الأشخاص وتستخدم أجهزة أو برمجيات حسب الفئة التي تندرج تحتها (فيزيائية أو سلوكيـــة) لغرض الحصول على قياسات أو تسجيلات لخصائص الشخص. ورغم أن تقنيات القياسات الحيوية تقيس خصائص مختلفة بطرق مختلفـــة، فإن نظم القياسات الحيويـــة تعتمد على نفس العمليـــات والتي يمكن تقسيمها إلى مرحلتين هما: التسجيـــل (Enrolment) وإثبات الهوية [8].



شكل 3: طريقة عمل القياسات الحيوية [4]

كما هو موضح في الشكل (3) فإن المزايا الفريدة للمستخدم تُستخرج من البيانات الحيوية الخام له، حيث تحول هذه البيانات إلى مجموعة صغيرة من البايت – للتخزين والمطابقة. هناك طرق مختلفة لاستخراج المزايا وبالتالي فإن المعالجة الاولية للبيانات الخام عادة ما تكون ضرورية. تقيس وحدة المطابقة مدى التشابه بين عينة المستخدم مع القالب المخزن في قاعدة البيانات، حيث توجد العديد من الطرق النموذجية للقياس والتي تعتمد على القياسات الاحصائية مثل: مقاييس المسافة، والتدابير، والشبكات العصبية، شجرة القرارات، النظرية الافتراضية، وتكون نتيجة القياس عادة عبارة عن نسبة تمثل الفرق بين العينتين بعد المطابقة [4].

بخلاف أنظمة المصادقة التقليدية، فإن نظام القياسات الحيوية لا يعطي إجابة نهائية ؛ بمعنى آخر، تتم عملية التحقق بناءً على مستوى التوافق بين النموذج المختبر مع النموذج المخزن مسبقاً [24].

نظام الـــ Biometric يعطي نتيجة التحقق بناءً على قيمة الخطـــأ المسموح به والمحددة مسبقاً للمستخدم، فإذا كانت النتيجة أقل من القيمة المسموح بها سيتم قبولها وإلا سيتم رفضها. التوازن المطلوب بين نوعين من الأخطاء: [24]

- النوع الأول: فشل النظام في التعرف على المستخدم الفعلي(False Rejection Rate) وتعني نسبة الرفض الكاذب واختصاره FRR ويحدد عن طريق حساب النسبة بين عدد المحاولات الشرعية المرفوضة / عدد المحاولات الشرعية.
- النوع الثاني: النظام يقبل مستخدم محتال (False Acceptance Rate) وتعني نسبة القبول الكاذب واختصاره FAR ويحدد عن طريق حساب النسبة بين عدد المحاولات الغير الشرعية المقبولة / عدد المحاولات الشرعية.

تطبيق القياسات الحيوية يعتمد المفاضلة بين النوعين من الأخطاء : حيث يجب أن يكون عدد الأخطاء في الحد الأدنى لكل من FARوFRR. وكما تم التوضيح سابقاً، فنظام الـــ Biometric يعطي نتيجة التحقق بناءً على قيمة الخطأ المسموح بها ، والتي تسمي أيضاً بشرط السماح وهو قيمة معينه من الخطاء مسموح بها للوصول للهدف وذلك للتماشي مع التغير الطبيعي، فالتسامح الكبير جدا يعطي نوع الخطأ الثاني (FAR)، والتسامح القليل جدا يعطي النوع الأول من الأخطاء (FRR). ولهذا تم اعتماد معدل الخطأ المتساوي كأفضل مقياس للمقارنة

(Equal Error Rate -ERR) وهو القيمة التي يتساوى فيها القبول الخاطئ مع الرفض الخاطئ[20] .

تطبيق ديناميكية ضغط المفاتيح يجب ان يراقب ايقاعات الكتابة للمستخدمين وتعلم الخصائص الفريدة التي يمكن استخدامها لوصف كل مستخدم، فكل فرد له سمات ثابتة ومختلفة، مثل مدة ضغطة المفاتيح، سرعة الطباعة والأوقات الفاصلة بين المفاتيح. احدى فوائد من استخدام هذا الأسلوب هو قدرته على رصد ضغطة الشخص بشكل نظامي وبسرية وبالتالي تحديد ما إذا كان له الصلاحية لاستخدام النظام او لا [19].

الخصائص السلوكية لديناميكية الضغط على لوحة المفاتيح

ديناميكية الضغط على لوحة المفاتيح هي المعلومات التفصيلية الزمنية التي تصف متى جرى الضغط على أي مفتاح ومتى جرى إطلاقه. تستخدم هذه المعلومات التفصيلية كوسيلة من وسائل التعرف على المستخدمين، حيث يقاس إيقاع خبط المفاتيح للمستخدم لبناء قالب حيوي مميز لنمط طباعة المستخدم من أجل التصديق المستقبلي. ويمكن تسجيل القياسات الخام المتاحة من معظم لوحات المفاتيح من أجل تحديد الخصائص التي سيتم استخدامها خلال مرحلة التحقق [6].

شكل 4: خصائص ديناميكية ضغط المفاتيح [16]

يوضح الشكل (4) ، الخصائص السلوكية لديناميكية الضغط على لوحة المفاتيح ، وذلك كالتالي:

- **Dwell time**: يسمى أيضاً Hold time وهو الزمن الذي يستغرقه المستخدم في الضغط على المفتاح وإطلاقه (زمن المكوث).
- **Flight time**: ويسمى أيضاً بزمن الطيران وهو الزمن الذي يأخذه المستخدم في الانتقال بين المفاتيح كالزمن بين رفع الإصبع عن المفتاح وضغط المفتاح التالي، أو الزمن بين ضغط الاصبع على المفتاح الاول ورفع المفتاح التالي وهكذا.
- **Total time**: الزمن الكلي المستغرق للطباعة.

إضافةً الى بعض الخصـــائص الأخرى مثل سرعة الطباعة، الأخطاء المتكـــررة وكيف يتم معالجتها بمفتاح (Backspace or Delete) والمفتاح المتداخلة عند استخدام مفتاح Shift.

اقترحت الدراسة التي أجريت في [24] تقسيم خصائص ضربات المستخدم على لوحة المفاتيح الي نوعين : منفصـــــلة عندما تكون الاحداث الزمنية غير متداخلة كزمن المكوث وزمن الطيران ، ومتصـــــلة عند تجميع كل الخصائص الزمنية كقيمة موحدة (الزمن الكلي)

الدراسات السابقة

سبيلاني أول من اقترح استخدام لوحة المفاتيح لتقييم ديناميكية ضغط الأفراد على لوحة المفاتيح للتحقق من هوية المستخدمين. في مرحلة التسجيل، يتم تسجيل معلومات الزمن الخاصة بالمستخدم عند طباعته لكلمة المرور باستخدام لوحة المفاتيح. بعد ذلك، يستطيع المستخدم الوصول إلى النظام عن كتابة طريق كلمة المرور، حيث سيتم مقارنة معلومات التوقيت لديناميكيات ضغطة المستخدم مع خصائصه المخزنة مسبقاً للتحقق من هويته[21] .

أجريت أول دراسة جدوى باستخدام الخصائص الزمنية لـــ Keystroke dynamics كأسلوب مصادقة من قبل جاينز عام 1980 في مؤسسة راند، حيث وضّح أن المدة الزمنية بين الضغط والإفراج عن مفتاح يسمى بزمن الانتظار Hold time او dwell time [13].

شهدت البحوث والدراسات السابقة اختلافاً فيما يتعلق بنوع الخصائص المستخلصة من سلوك المستخدمين أثناء طباعة كلمة المرور .ا لدراسة التي أُجريت في [17] استخدمت زمن الانتظار (Hold time) وزمن الطيران في حالة افلات المفاتيح (الزمن بين افلات المفتاح الاول والثاني). وقد أظهرت الدراسة التي أجريت في [7] [9],[14] أن استخدام كلٍ من زمن المكوث وزمن الطيران يعطي نتائج أفضل من استخدام خاصية واحدة فقط .

ومع ذلك أظهرت الدراسة التي أُجريت في [23]،[25] أن زمن الطيران (Flight time) بين ضغطات المفاتيح يشهد تبايناً عالياً بالمقارنة مع زمن الانتظار. وقد رجحّ الكاتب السبب في ذلك الى اختلاف التفاعل بين الأفراد على لوحة المفاتيح. على سبيل المثال، زمن الطيران بين المفاتيح للشخص الذي يستخدم أصبع واحد أو أثنان أعلى من ذلك الذي يستخدم الأصابع العشرة في الطباعة.

الجدير بالذكر أن زمن الطيران أو ما يطلق عليه بزمن التأخير (Time latency) هو أحد السمات الأكثر استخداماً في العديد من الدراسات السابقة، ويمكن التعبير عنه بثلاثة أشكال: المدة بين الضغط علي مفتاح معين وضغط المفتاح التالي (Press-Press)؛ المدة بين إفلات مفتاح معين إفلات المفتاح التالي RR(Release-Release)، المدة بين إفلات مفتاح معين وضغط المفتاح التالي RP(Release-Press)، يطلق على الزمن PP أيضاً Digraph [16] . وقد حددت الدراسة التي أجريت من قبل [22] الحالة النفسية للمستخدم باستخدام زمن المكوث (dwell time).

يعتمد أداء خوارزميات التصنيف على قياس مدى التشابه والاختلاف بين خصائص البيانات الحيوية للمستخدمين وقوالب خصائصهم المستخلصة مسبقاً ، حيث تتم مصادقة المستخدمين اعتماداً على وجود هذه الخصائص ضمن حدود التسامح المحددة مسبقاً[11]. هناك العديد من التقنيات المستخدمة في التصنيف مثل الشبكات العصبية و الطرق الإحصائية (المتوسط، والمسافة الإقليدية لكل العينات، مستوى الانحراف المعياري).

وفي دراسة تم القيام بها في [5] تم فحص أداء keystroke dynamics باستخدام PIN (رقم التعريف الشخصي) بأطوال مختلفة باستخدام خوارزمية الوزن حيث تفاوتت نسبة معدل الخطأ FAR ما بين (0.13% الى 0.28%) باستخدام مسافة Manhattan بين قوالب الخصائص السلوكية للمستخدمين (biometric template) والبيانات المختبرة، في حين سجلت الدراسة التي أجريت في [21] نتيجة أفضل لخوارزمية التصنيف وصلت الى 75%.

في تجربة تم القيام بها في [20] كانت الدعوة موجهة إلى خمسة عشر مستخدماً للضغط على ثلاث كلمات سر الأكثر شيوعاً خمس مرات باستخدام نفس لوحة المفاتيح بحيث كانت كلمة السر الأولى مكونة من أرقام فقط ("123456") والثانية مكونة من مجموعة حروف ("password") والثالثة مزيج من الأثنين معاً (kolkata123).

أظهرت الدراسة [20] الحصول على أفضل نتيجة عند كتابة المستخدمين لنص ثابت (kolkata123) وقد رجح الكاتب السبب في ذلك بأن المستخدمين اعتادوا مسبقاً على الضغط على كلمة المرور (kolkata123) للحصول على اسلوب كتابة مميز وأستنتج أيضاً بأن طول سلسة كلمة المرور هي أحد العوامل التي تختلف بشكل كبير بين مختلف المستخدمين، اي أن كلمات المرور ذات التسلسل القصير تقود الى أداء إحصائي بأسلوب كتابة سيئ. وصلت هذه التجربة لأقل معدل خطأ EERعند كلمة المرور (kolkata123) يصل الى (0.133) وكلمة المرور الثانية ("password") بقيمة (0.4) والثالثة ("123456") الى (0.53) على التوالي .

تؤكد الدراسات السابقة أهمية استخدام ديناميكية ضغطات لوحة المفاتيح (Keystroke dynamics) كحل إحصائي جدري يمكن توظيفه بفعالية الى جانب كلمات المرور للتحقق من هوية المستخدمين.

من الواضح ان استخدام Keystroke Dynamics في التحقق من الهوية يعتبر اسلوب فعال وسهل عند استخدامه كعامل ثاني للتحقق من الهوية مع كلمات المرور، ولكن عملية استخدام هذه الأداة للوصول الى قالب مثالي يمثل المستخدم تعتبر صعبة وذلك لأن خوارزميات التصنيف مختلفة واختلاف نوع كلمة المرور في الدراسات مختلفة و عدد العينات أثناء مرحلة التسجيل مختلفة .

ومن هنا تظهر أهمية هذه الدراسة ، في تحديد دور نوع كلمة المرور بدرجات تعقيد مختلفة للوصول لقالب مثالي فريد يمثل المستخدم ويميزه عن غيره من المستخدمين، وتجعل خصائصه السلوكية أكثر استقرارا

منهجيـــــة الدراسة

تهدف هذه الدراسة الى تحديد نوع كلمة المرور التي تجعل خصائص المستخدم السلوكية أكثر استقراراً وبالتالي تعزيز درجة أمان كلمات المرور في المصادقة الالكترونية. لذا تم تطوير تطبيق برمجي لغرض إجراء تجربة على مجموعة من المستخدمين لمحاكاة مرحلة التسجيل على ثلاث مراحل :

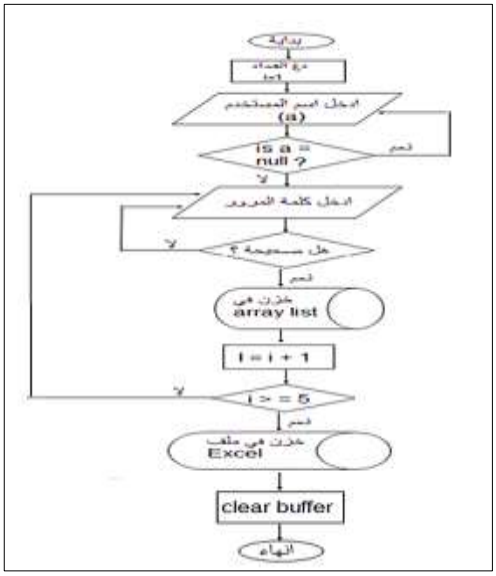
- المرحلة الأولى: التسجيل باستخدام كلمة مرور بسيطة (أرقام فقط).
- المرحلة الثانية :التسجيل باستخدام كلمة مرور متوسطة التعقيد(حروف صغيرة).
- المرحلة الثالثة: التسجيل باستخدام كلمة مرور معقدة (حروف صغيرة وكبيرة وأرقام).

حيث يتم تسجيل جميع الاحداث الزمنية لتفاعل المستخدمين مع لوحة المفاتيح وتحليل الخصائص المختلفة لهم من أجل تحديد نوع كلمة المرور التي تكون فيها خصائص الـــ keystroke dynamics للمستخدمين أكثر وضوحاً.

تقتضي الخطة المقترحة للإجابة على تساؤلات هذه الدراسة إجراء تجربة عن طريق تطوير تطبيق برمجي لبناء منصة

متكاملة يتم من خلالها جمع معلومات المستخدم السلوكية أثناء تفاعله مع لوحة المفاتيح.

1. يطلب من المستخدمين في المرحلة الأولى تسجيل اسمائهم ومن ثم طباعة كلمات المرور المعروضة على الشاشة، حيث يتم في المرحلة الأولي تسجيل أول كلمة مرور بسيطة مكونة من أرقام فقط وهي (123456) وذلك لاختبار مدى تأثير كلمات المرور على سلوك المستخدم أثناء الطباعة
2. المرحلة الثانية يتم فيها التسجيل باستخدام كلمتي مرور مختلفة التعقيد احداهما كلمة مرور متوسطة مكونة من حروف وأرقام وهي (kolkata123) والتي تم اختيارها من الدراسة التي اجريت في [20] ، حيث تم أيضا من خلالها استنباط كلمة مرور المعقدة والتي لم يتم أخدها بعين الاعتبار في تلك الدراسة وهي (KolKatA123). الخوارزمية التالية توضح الخطة المقترحة لتنفيذ التجربة البرمجية لتجميع الخصائص السلوكية للمستخدمين أثناء تفاعلهم مع لوحة المفاتيح .



شكل 5: خوارزمية تجميع خصائص للمستخدمين

تتطلب الدراسة جمع المعلومات السلوكية لضربات المستخدم على لوحة المفاتيح، وذلك بعد موافقة المستخدم على إجراء التجربة وإتباع التعليمات اللازمة ليتمكن من التسجيل بصورة واضحة [20].

الخصائص التنفيذية للتجربة

- **عدد المستخدمين**

بما أن الدراسة تتطلب بجمع المعلومات السلوكية لضربات المستخدم على لوحة المفاتيح، فإن ذلك يتم بعد موافقة المستخدم على إجراء التجربة وإتباع التعليمات اللازمة ليتمكن من التسجيل بصورة واضحة، وقد تم تطبيق التجربة على خمسة عشر مستخدماً من طلاب وطلبة وأعضاء هيئة تدريس بكلية تقنية المعلومات

- **عدد مرات التسجيل**

عند محاكاة المستخدم لمرحلة التسجيل يكون مطلوباً منه تسجيل بياناته(كاسم المستخدم، وكلمات المرور المعروضة) ويكون عدد مرات تسجيل كلمات المرور في كل مرحلة (خمس مرات) اعتماداً على الدراسة التي أجريت في [20].

النتائج والمناقشة

تم تسجيل معلومات ضغط المفاتيح (أحداث ضغط المفاتيح وطابعها الزمني)، أثناء كتابة كلمات المرور في ورقة انتشار (csv file). والتي ينم فتحها باستخدام برنامج excel . وبما أن التجربة قد أجريت بواسطة 15 مستخدم هذا يعني أن كل مستخدم لديه ملفين توضح معلوماتهم السلوكية (keystroke dynamics) خلال تطبيقهم عملية التسجيل لمرحلتين . وبالنظر إلى حقيقة أنه تم تطبيق التجربة مع 15 مشاركا، فقد تم إنتاج ما يعادل 30 ملفا ، وبهذا تكون التجربة قد أنتجت معلومات مفيدة حول تفاعل المستخدم مع تطبيق التسجيل. ولهذا يجب تحديد البيانات أكثر أهمية من البيانات الخام لتحليلها ، والطريقة التي سيتم استخراج ميزات ضغط المفاتيح منها . تصف البنود الفرعية التالية خطة تحليل البيانات استنادا إلى المعلومات التي تم الحصول عليها من كل تصف البنود الفرعية التالية خطة تحليل البيانات استنادا إلى المعلومات التي تم الحصول عليها من كل سيناريو.

- **المعالجة المسبقـــــة للبيانات**

بعد جمع البيانات الأولية (الخام)، لوحظ أن للمستخدمين سلوكيات مختلفة عند الكتابة على لوحة المفاتيح، وباختلاف درجة تعقيد كلمات المرور المستخدمة في تجربة الدراسة ، أظهر أغلب المستخدمين اختيارهم لمفتاح الحروف الكبيرة Caps Lock عند طباعة الحروف الكبيرة ، في حين استخدم بعضهم مفتاح الإزاحة shift. وبما أن البيانات الأولية تحتوي على الطابع الزمني لسلوك كتابة المستخدم، فمن الضروري معالجتها لاستخراج الخصائص الزمنية لـــ keystroke dynamics لهم . البند التالي يوضح ماهية الخصائص المستخلصة من بيانات المستخدمين

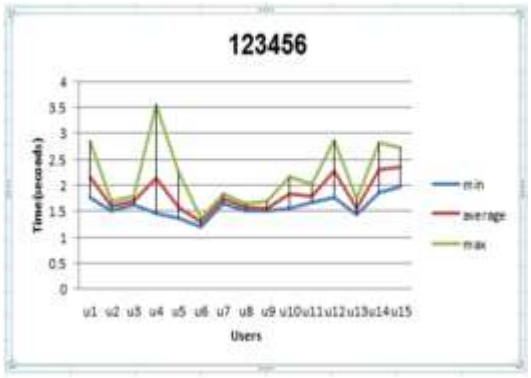
- **الخصائص المستخلصـــــــة**

في هذه الدراسة ، تم استخلاص خصائص كل من زمن المكوث (dwell time)، وزمن الطيران (flight time) ، والزمن الكلي المستغرق في طباعة كلمة المرور (total time)، إلا ان الطريقة المتبعة في استخراج زمن المكوث في هذه الدراسة تختلف عن ما تم في الدراسات السابقة نظراً لتوظيف كل من مفتاحي الحروف الكبيرة(caps Lock) والازاحة (shift), كعناصر أساسية لإنتاج الحروف الكبيرة . بمعنى أخر، تم دمج خصائص الـــ caps lock مع خصائص الحرف الزمنية كخاصية موحدة لإنتاج الحرف الكبير ، ونفس الامر قد تم اعتماده عند استخدام مفتاح shift.

لتوضح ماهية الخصائص المستخلصة من بيانات المستخدمين تم تحليل النتائج بناء على الخطة التحليلية كالتالي:

- تحليل النتائج المتصلة بالخصائص السلوكية للمستخدمين عند طباعة كلمة المرور البسيطة (123456).
- تحليل نتائج طباعة المستخدمين لكلمة المرور الثانية (kolkata123) لخصائصهم السلوكية.
- دراسة خصائص المستخدم السلوكية على لوحة المفاتيح عند طباعة كلمة المرور المعقدة (KolKatA123).

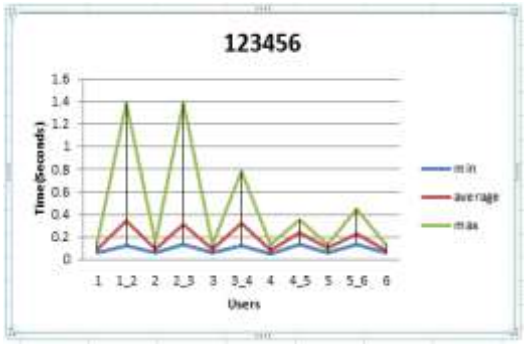
يوضح الشكل التالي مستوى تباين خصائص المستخدمين المتصلة عند طباعتهم لنفس كلمة المرور البسيطة (123456).



شكل 6: الخصائص المتصلة للمستخدمين (كلمة المرور البسيطة)

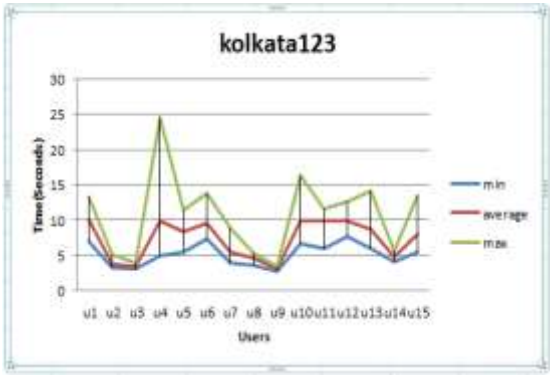
كما هو موضح من الشكل (6)، يبين المحور الافقي للمستخدمين (U1 to U15) ويشير المحور العمودي الزمن الكلي لخصائصهم المتصلة المقاس بالثانية . كما هو واضح من الشكل ، فخصائص المستخدمين المتصلة أظهرت نوعاً من التفاوت عند طباعتهم لنفس كلمة المرور البسيطة ، وهذا يثبت أنه لكل مستخدم خصائصه السلوكية التي تميزه. يتضح من الشكل أيضاً مستوى التقارب لخصائص المستخدمين المتصلة باتجاه المتوسط الحسابي، ويظهر ذلك بوضوح لدى المستخدمين (U2,U3,U6,U7,U8,U9,U13) الذين اظهروا أيضاً تشابهاً متقارباً لخصائصهم السلوكية المتصلة. ويرجع السبب في ذلك أن كلمة المرور بسيطة جداً وبإمكان المستخدم طباعتها بسهولة . بخلاف ذلك ، اظهرت النتائج اختلافا واضحاً في خصائص باقي المستخدمين (U1,U4,U5,U10,U11,U12,U14,U15) والناتج من تباين مهارتهم على لوحة المفاتيح;العامل الذي يجب أخذه بعين الاعتبار عندما يتعلق الأمر بتمييز المستخدمين عن بعضهم.

بالنظر لخصائص المستخدمين المنفصلة كما في شكل(7)، والمتمثلة في زمن الطيران (Flight time) ، زمن المكوث (Dwell time) عند طباعة المستخدمين لكلمة المرور البسيطة، يتضح مدى التباين لزمن الطيران مقارنة بزمن المكوث ، الامر الذي يثبت أن زمن المكوث أكثر استقراراً من زمن الطيران . مستوى التباعد المتفاوت لقيم الخصائص المنفصلة لأغلب المستخدمين يدل على صعوبة تمييز هم عند طباعة كلمة المرور البسيطة ، الأمر الذي قد يعيق عملية التحقق من هويتهم.



شكل 7: الخصائص المنفصلة للمستخدمين (كلمة المرور البسيطة)

كما يوضح الشكل (8) مستوى تباين المستخدمين المتصلة عند طباعتهم لنفس كلمة المرور متوسطة التعقيد (kolkata123).

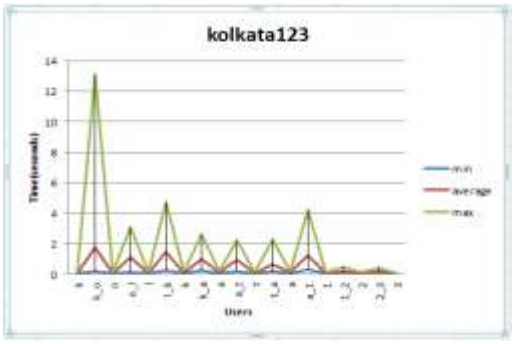


شكل 8: الخصائص المتصلة للمستخدمين (كلمة المرور متوسطة التعقيد)

كما هو واضح من الشكل (8)، فإن خصائص المستخدمين المتصلة سجلت تبايناً ملحوظاً لدى أغلب المستخدمين (U1,U4,U5,U6,U7,U10.U11,U12,U13,U15)، الذين أظهرت نتائجهم انحرافاً عالياً عن المتوسط مقارنة بباقي المستخدمين ، وإن دل ذلك على شيء ، فإنه بدل على عدم استقرار الخصائص السلوكية للمستخدمين باختلاف مهارتهم الكتابية على لوحة المفاتيح.

وعند مقارنة هذا المستوى مع مستوى تباين المستخدمين عند طباعة كلمة المرور البسيطة تبين أن بعض المستخدمين حافظوا على مستوى التباين لديهم باختلاف نوع كلمة المرور (U2,U3,U9) وهذا يعني أن كفاءة هؤلاء المستخدمين على لوحة المفاتيح عالية نسبياً.

كذلك بالنسبة للخصائص المنفصـــــلة ، يمكن توضيح مستوى التباين لخصائصها ل 15 مستخدم من الشكل (9):

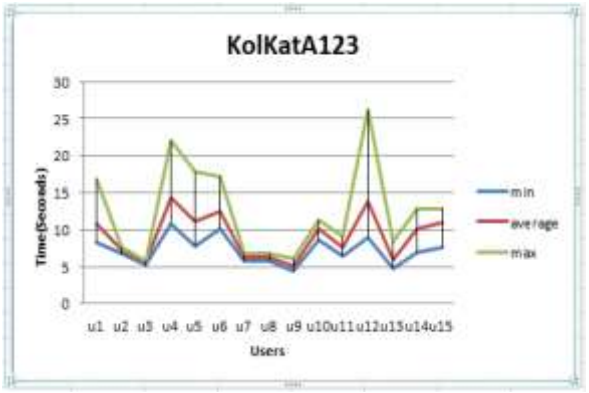


شكل 9: الخصائص المنفصلة للمستخدمين (كلمة المرور متوسطة التعقيد)

عند دراسة الخصائص المنفصلة للمستخدمين عند طباعة كلمة المرور متوسطة التعقيد ، تبين استقرار زمن المكوث وتباين زمن الطيران . وقد تم الوصول الى هذه النتيجة أيضاً عند توظيف كلمة المرور البسيطة ، وهذا يثبت ويؤكد ما توصلت اليه الدراسات السابقة [15]. عند مقارنة تباين الخصائص المنفصلة والمتصلة، يتبين ان استخدام الخصائص المتصلة يعطي صورة أوضح لمدى اختلاق المستخدمين مقارنة بالخصائص المنفصلة ، التي اظهرت تبايناً متساويا لأغلب قيمها باختلاف مكوناتها.

لذا ، يمكن إستخلاص أن الخصائص المنفصلة تعطي تمييزاً واضحاً بين المستخدمين مقارنة مع الخصائص المنفصلة عند توظيف كلمة المرور متوسطة التعقيـــــد.

أظهرت نتائج الجلسة الأخيرة للتجربة أن خصائص السلوكية المتصلة تفاوتت باختلاف المستخدمين، وهذا يدل على تباين سلوكهم عند طباعة كلمة المرور المعقدة . يتضح من الشكل (10) أن معدل انحراف خصائص المستخدمين عن المتوسط منخفض نسبيا لدى أغلب المستخدمين ، وهذا يدل على ان قيم خصائصهم المتصلة لم تشهد تغيراً كبيراً خلال مرحلة التسجيل.

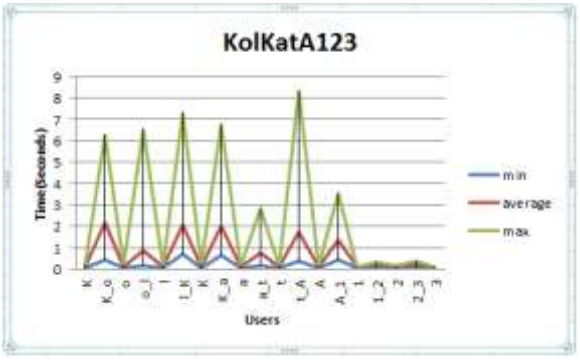


شكل 10: الخصائص المتصلة للمستخدمين (كلمة المرور المعقدة)

عند مقارنة مستوى التباين بين خصائص المستخدمين، أظهرت قيم الخصائص المتصلة للمستخدمين (U1,U4,U5,U6,U7,U10,U14,15) انحرافا عاليا عن المتوسط مقارنة مع باقي المستخدمين ، الذين أظهرت خصائصهم تقارباً ملحوظاً من قيم المتوسط .

وعند مقارنة هذا المستوى مع مستوى تباين المستخدمين عند طباعة كلمة المرور البسيطة, والمتوسطة التعقيد، تبين أن بعض المستخدمين حافظوا على مستوى التباين لديهم باختلاف نوع كلمة المرور (U2,U3,U9) ، وهذا التباين ناتج من سرعة طباعتهم على لوحة المفاتيح اي أن كفاءة هؤلاء المستخدمين على لوحة المفاتيح عالية نسبياً.

يمكن توضيح مستوى التباين لخصائص المنفصلة ل 15 مستخدم عند طباعة كلمة المور المعقدة للمرة الأولى من الشكل (11)



شكل 11: الخصائص المنفصلة (كلمة المرور المعقدة)

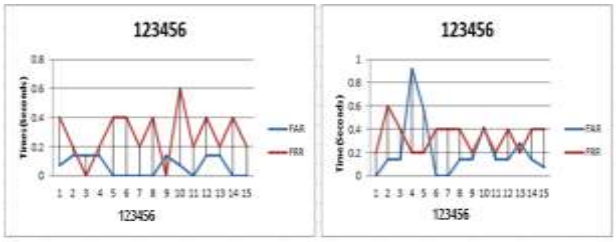
- **خوارزمية التصنيف**

في هذه الدراسة تم الاعتماد على الخوارزميـــــــة المقترحة في الدراسة [26]، والتي تم توظيفها أيضاً في [22]. تعتمد هذه الخوارزمية على المتوسط والانحراف المعياري للبيانات. تعمل هذه الخوارزمية على النحو التالي: إذا كانت البيانات المختبرة تقع ضمن المتوسط والانحراف المعياري للمعلومات المخزنة، يتم زيادة عدد المطابقات بمقدار 1. والتي يتم حساب متوسطها واستنادا إلى قيمة التسامح المخصصة، يتم اتخاذ القرار. على سبيل المثال، اقترح [26]أنه إذا كان متوسط الخصائص يساوي أو أكبر من 75٪، يتم قبول المستخدم. وإلا رفضت المحاولة. وبخلاف ذلك، فقد اعتمدت هذه الدراسة على تخصيص قيمة التسامح وفقاً للمستخدمين باختلاف نوع كلمة المرور والزمن الذي استغرقه كلٍ منهم في الطباعة بتطبيق خوارزمية التصنيف على بيانتهم الأولي، ثم اختيار القيمة الأكثر تكراراً او متوسط القيم . اعتماداً على قيمة التسامح (threshold value) لكل مستخدم ، يتم قياس أداء خصائص المستخدمين لتحديد قيم كلٍ من FAR,FRR.

وباعتبار المحاولة الاولى لكل مستخدم لطباعة كلمات المرور الثلاثة كمحاولة غير مشروعة لخصائص مستخدم ما ، تم حساب قيمة FAR. هذا يعني ان لكل مستخدم 14 محاولة غير مشروعة تمثل المرة الاولى التي قام بها المستخدمين بطباعة كلمة المرور سواء كانت (بسيطة ، متوسطة التعقيد، معقدة).

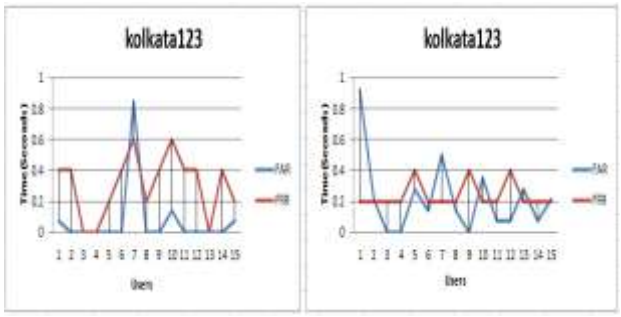
من جانبٍ أخر، تم حساب FRR باختبار مدى وقوع قيم خصائص المستخدمين (المتصلة والمنفصلة) والتي تم استخراجها خلال مرحلة التسجيل من قيم التسامح المحددة مسبقاً . وهذا يعني ان لكل مستخدم خمسة محاولات مشروعة يتم على اساسها تحديد قيم FRR للمستخدمين . الجدير بالذكر أن أفضل أداء للخوارزمية يظهر ERR والذي يمثل الوضع الذي تتطابق فيه FRR,FAR.

توضح الاشكال التالية أداء خوارزمية التصنيف لقيم كلٍ من FAR,FRR للخصائص المنفصلة والمتصلة المتعلقة بكلمات المرور الثلاثة.



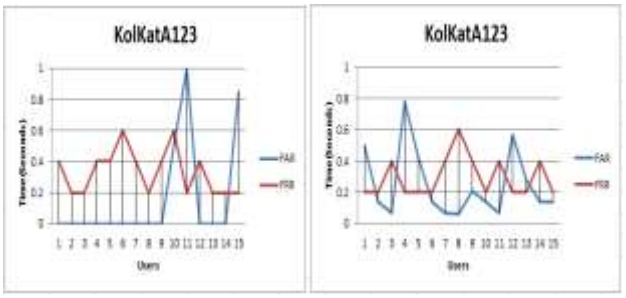
شكل(12): كلمة المرور البسيطة

يظهر الشكل (12) تطبيق خوارزمية التصنيف على الخصائص المنفصلة(الجانب الايسر) والمتصلة(الجانب الايمن) لكلمة المرور البسيطة. أظهرت النتائج قيماً لـــ FAR تفاوتت تبين 0%–0.25 % عنج استخدام الخصائص المنفصلة ،في حين تباينت قيم FRR بين 0%–0.6 ولم يحصل تطابق لقيمها الا في حالتين فقط ــ حيث وصلت قيمة ERR لـــ 0%. من جانبٍ آخر ــ أظهرت نتائج تطبيق الخوارزمية على الخصائص المتصلة تحسناً ملحوظا لدى معظم المستخدمين ــ حيث تم الوصول الى قيمٍ لـــ EER تفاوتت بين 0.1%–0.3% لمعظم المستخدمين .و هذا يؤكد افضلية استخدام الخصائص المتصلة عند استخدام كلمة المرور البسيطة.



شكل(13): كلمة المرور المتوسطة

يوضح شكل 13 أداء خوارزمية التصنيف على الخصائص المنفصلة (الجزء الايسر) والخصائص المتصلة (الجزء الايمن) عند كتابة كلمة المرور متوسطة التعقيد . كما هو واضح من الشكل، تبين أن قيم FAR, FRR تفاوتت عند اغلب المستخدمين عند استخدام الخصائص المنفصلة بين 0%–0.9% ولم يظهر اي تطابق لقيم الخطأين (ERR)، الامر الذي يجعل استخدام الخصائص المنفصلة غير مرضياً بالنسبة لكلمة المرور متوسطة التعقيد . خلافاً لذلك ، أظهرت نتائج الخصائص المتصلة أداءً أفضل ، حيث تم الحصول على أقل EER بقيمـــــة 0.2%.



شكل(14): كلمة المرور المعقدة

يوضح شكل 14 أداء الخصائص السلوكية المرتبطة بكلمة المرور المعقدة باستخدام الخصائص المنفصلة(الجانب الايسر) والخصائص المتصلة(الجانب الأيمن) . أظهرت الخوارزمية نتائج أفضل عند استخدام كلمة مرور معقدة مقارنة بكلمات المرور السابقة، وذلك بسبب التباين المرتفع بين سلوكيات المستخدمين، حيث لم تتجاوز قيم FAR,FRR لـــ 0.8% عند استخدام الخصائص المنفصلة ، إضافة الى عدم ظهور ERR لدى معظم المستخدمين . خلافاً لذلك فقد أظهر استخدام الخصائص المتصلة نتائج أفضل مقارنة بالخصائص المنفصلة حيث لم تتجاوز قيم FAR, FRR 0.6 و 0.8 على الترتيب مع تطابق قيمهما(ERR) لدى معظم المستخدمين.

يمكن تلخيص نتائج الدراسة في الآتي

- أكدت نتائج الدراسة أن خاصية زمن المكوث dwell time أكثر استقراراً من زمن الطيران مهما كان نوع كلمة المرور المستخدمة.
- أن استخدام كلمة المرور المتوسطة التعقيد والمعقدة أفضل مقارنة بكلمة المرور البسيطة.
- استخدام الخصائص المتصلة أظهر استقراراً ملحوظاً لسلوكيات المستخدمين على لوحة المفاتيح باختلاف نوع كلمة المرور.
- أظهرت النتائج أن استخدام الخصائص المتصلة المرتبطة بكلمة المرور المعقدة هو أفضل لتمييز المستخدمين عن بعضهم ، مع الاخذ بعين الاعتبار سلوكيات المستخدمين لتوليد الحروف الكبيرة والأرقام

الخلاصة

في هذه الدراسة ، تم تسليط الضوء على المصادقة الالكترونية (التحقق من الهوية) ، والتطرق بشكل موسع الى استخدام ديناميكية الضغط على لوحة المفاتيح كأحد الأساليب التي يمكن اعتمادها كمعامل إضافي لتعزيز مستوى الأمن الذي توفره كلمات المرور. هدفت هذه الدراسة الى تحديد ماهية الخصائص ونوع كلمة المرور التي تجعلها أكثر استقراراً وتفرداً . تم إجراء تجربة لتجميع خصائص المستخدمين بتطوير تطبيق برمجي بلغة الجافا يخدم هذا الغرض، حيث تم تجميع الخصائص السلوكية للمستخدمين أثناء تعاملهم مع لوحة المفاتيح لطباعة ثلاث كلمات مرور بدرجات تعقيد مختلفة . تم بموجب هذه التجربة تجميع البيانات الاولية ومعالجتها لاستخلاص الخصائص اللازمة للتقييم.

عند دراسة الخصائص المنفصلة للمستخدمين تبين مدى التباين المرتفع لها عن المتوسط ، وهذا يدل على اختلاف سلوكيات المستخدمين عند طباعة كلمة المرور المعقدة للمرة الأولى باختلاف مهاراتهم الكتابية على لوحة المفاتيح ، وباختلاف درجة تعقيد كلمات المرور المستخدمة في التجربة ، أظهر أغلب المستخدمين اختيارهم لمفتاح Caps Lock (مفتاح الحروف الكبيرة) لطباعة الحروف الكبيرة ، في حين استخدم بعضهم مفتاح shift (مفتاح الإزاحة). وبنفس الكيفية تباين سلوك المستخدمين بين استخدام لوحة الارقام بالضغط على NumLk(مفتاح تفعيل لوحة الارقام) ومفاتيح الارقام أعلى مفاتيح الحروف. جميع هذه المعايير تضيف مزيداً من التفرّد لخصائص المستخدمين المنفصلة.

تتمثل أفاق التطوير في تطبيق التجربة على نطاق موسع من المستخدمين للحصول على بيانات أولية شاملة ونتائج أكثر دقةً نظرا لاقتصار التجربة في هذه الدراسة على 15 مستخدماً الأمر الذي يحد من تعميم نتائج الدراسة. كما يمكن دراسة مدى استقرار خصائص المستخدمين السلوكية باختلاف حالتهم الصحية و نوع لوحة المفاتيح المستخدمة

المراجع

[1]- القحطاني، خالد بن سليمان و الغثبر، محمد بن عبدالله، (2009) ، أمن المعلومات، الطبعة الأولى

[2]- المهنا، نورا.2011 استخدام مجموعة المصنّفات لمصادقة التوقيع الديناميكي. Communications of the ACS، 4(2).

[3]- العطاس، إيمان و مسحول ، سهام . 2012، اختيار السمات في مصادقة التواقيع الديناميكية.Communications of the ACS, 5(1) .

[4]- ما هي القياسات الحيوية (White paper)
http://www.aware.com/wp-content/uploads/2016/02/WP_What-are-Biometrics_Arabic_0216.pdf Access date [21/4/2020]

[5]- Abualgasim, S.D. and Osman, I. (2011), An application of the keystroke Dynamics biometric for securing PINs and passwords , WCSIT, 1(9), pp 398-404

[6]- Alsultan, A., Warwick, K. and Wei, H., 2016. Free-text keystroke dynamics authentication

p. 149-162. In International Conference on Innovative Computing and Communications . Springer, Singapore.

[20]- Roy, S., Roy, U. and Sinha, D.D., 2014. Enhanced knowledge-based user authentication technique via keystroke dynamics. Int. J. Eng. Sci. Invention (IJESI), 3(9): 41-48.

[21]- Sachan, M., Joshi, P. and Raul, N., 2017, September. Keystroke Dynamics Support for Authentication.p. p. 186-191. In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). IEEE

[22]- Shanmugapriya, D. and Ganapathi, P., 2019. A Framework for Improving the Accuracy of Keystroke Dynamics-Based Biometric Authentication Using Soft Computing Techniques.p. 208-235. In Biometric Authentication in Online Learning Environments .IGI Global.

[23]- Shute, S., Ko, R.K. and Chaisiri, S., 2017, August. Attribution Using Keyboard Row Based Behavioural Biometrics for Handedness Recognition. p.1131-1138.In 2017 IEEE Trustcom/BigDataSE/ICESS .IEEE

[24]- Sundararajan, A., Sarwat, A.I. and Pons, A., 2019. A survey on modality characteristics, performance evaluation metrics, and security for traditional and wearable biometric systems. ACM Computing Surveys (CSUR), 52(2): pp.1-36

[25]- Syed, Z., Banerjee, S. and Cukic, B., 2016. Normalizing variations in feature vector structure in keystroke dynamics authentication systems. Software Quality Journal, 24(1):137-157.

[26]- Yan, Jing. 2009, Continuous authentication based on computer security , Master's thesis, lulea university,Sweden

for Arabic language. IET Biometrics, 5(3):164-169

[7]- Ali, M.L., Monaco, J.V., Tappert, C.C. and Qiu, M., 2017. Keystroke biometric systems for user authentication. Journal of Signal Processing Systems, 86(2-3):175-190

[8]- Bhartiya, N., Jangid, N. and Jannu, S., 2018, April. Biometric Authentication Systems: Security Concerns and Solutions. p. 1-6. In 2018 3rd International Conference for Convergence in Technology (I2CT). IEEE

[9]- Bhardwaj, I., Londhe, N.D. and Kopparapu, S.K., 2017. A novel behavioural biometric technique for robust user authentication. IETE Technical Review, 34(5):pp.478-490.

[10]- Calot, E.P., Ierache, J.S. and Hasperué, W., 2019, September. Document Typist Identification by Classification Metrics Applying Keystroke Dynamics Under Unidealised Conditions.p. 19-24. In 2019 International Conference on Document Analysis and Recognition Workshops (ICDARW) . IEEE

[11]- Conijn, R., Roeser, J. and van Zaanen, M., 2019. Understanding the keystroke log: the effect of writing task on keystroke features. Reading and Writing, 32(9): 2353-2374.

[12]- Chatterjee, K., 2019. Biometric re-authentication: an approach towards achieving transparency in user authentication. Multimedia Tools and Applications, 78(6): 6679-6700.

[13]- Fouad, K.M., Hassan, B.M. and Hassan, M.F., 2016. User authentication based on dynamic keystroke recognition. International Journal of Ambient Computing and Intelligence (IJACI), 7(2):1-32

[14]- Kozierkiewicz-Hetmańska, A., Marciniak, A. and Pietranik, M., 2016, September. User Authentication Through Keystroke Dynamics as the Protection Against Keylogger Attacks.p. 345-355. In International Conference on Computational Collective Intelligence (). Springer, Cham.

[15]- Migdal, D. and Rosenberger, C., 2019, July. Keystroke Dynamics Anonymization System. ICETE (2): 448-455

[16]- Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y., 2018. Multi-factor authentication: A survey. Cryptography, 2(1): 1.

[17]- Obaidat, M.S., Krishna, P.V., Saritha, V. and Agarwal, S., 2019. Advances in Key Stroke Dynamics-Based Security Schemes.p.165-187. In Biometric-Based Physical and Cybersecurity Systems .Springer, Cham.

[18]- Quraishi, S.J. and Bedi, S.S., 2018, November. Keystroke Dynamics Biometrics, A tool for User Authentication–Review.p. 248-254. In 2018 International Conference on System Modeling & Advancement in Research Trends (SMART). IEEE

[19]- Raul, N., Shankarmani, R. and Joshi, P., 2020. A Comprehensive Review of Keystroke Dynamics-Based Authentication Mechanism.