Chapter 4

A Survey of Machine Learning Techniques for Behavioral-Based Biometric User Authentication

Nurul Afnan Mahadi,
Mohamad Afendee Mohamed,
Amirul Ihsan Mohamad, Mokhairi Makhtar,
Mohd Fadzil Abdul Kadir and Mustafa Mamat

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.76685

Abstract

Authentication is a way to enable an individual to be uniquely identified usually based on passwords and personal identification number (PIN). The main problems of such authentication techniques are the unwillingness of the users to remember long and challenging combinations of numbers, letters, and symbols that can be lost, forged, stolen, or forgotten. In this paper, we investigate the current advances in the use of behavioral-based biometrics for user authentication. The application of behavioral-based biometric authentication basically contains three major modules, namely, data capture, feature extraction, and classifier. This application is focusing on extracting the behavioral features related to the user and using these features for authentication measure. The objective is to determine the classifier techniques that mostly are used for data analysis during authentication process. From the comparison, we anticipate to discover the gap for improving the performance of behavioral-based biometric authentication. Additionally, we highlight the set of classifier techniques that are best performing for behavioral-based biometric authentication.

Keywords: continuous authentication, behavioral biometric, machine learning, classification, clustering

1. Introduction

Over the past decade, the field of computer security has evolved along with the changing nature of technology. Computer security comprises of measures and controls that ensure the goals of information security that are confidentiality, integrity, and availability, defined over hardware, software, firmware, and information being processed, stored, and communicated,

are achieved [1]. These goals of information security, also known as CIA triad, is a benchmark model used to evaluate the physical, logical, and perceptual security of information in an organization [2, 3]. The elements of the triad are considered as the three most crucial components of information security. It can have serious effects for an organization if any one of this triad is breachable.

Confidentiality is roughly equivalent to privacy or secrecy which offers prevention of the sensitive information from disclosure by unauthorized individuals or systems [4]. By and large, it is also the one which is attacked most often. Cryptography via encryption algorithms is commonly used to ensure the confidentiality of data in storage or transferred from one computer to another.

Integrity is typically described as the trustworthiness, accuracy, and consistency of data in which the data itself cannot be altered or modified undetectable by unauthorized user [4]. Cryptography plays a major role in ensuring data integrity. This is done by hashing the original data and transmitting the data and the hash to the recipient followed by another hashing on the received data and comparison with the received hash to verify its integrity.

Availability is defined as the security controls required to ensure that the information concerned is readily accessible to the authorized parties when they request it [1]. Denial of service (DoS) attack can be a good example of many threats to this security controls. DoS renders the system to an unavailable state to serving legitimate request by making the server fully utilized the processing power, bandwidth, and memory to handle request mostly mounted by this attack.

Last but not least, authentication is a key point to provide effective information security. Authentication process verifies the identity of a user, process, or device and allows only legal users to use the resources and services in an authorized manner while denying all illegal ones [1].

Nowadays, user authentication is an issue and thus a challenge that becomes more important than ever before [5]. For an online banking system, it is very important to secure the users' accounts and protect their assets and personal information from malicious hands due to highly sensitiveness of data held inside. There are many existing authentication methods; in general, they are categorized into knowledge-based method, possession-based method, and biometric-based method. For sure, all of the methods have their own uniqueness (strengths and weaknesses); however, the environment determines which authentication approach is best suited.

When talking about the authentication in general, two types of well-known approaches have been proposed in the literature, namely, continuous authentication approach and static authentication approach [6]. Continuous authentication approach which can also be acknowledged as dynamic authentication verifies users repeatedly throughout the entire session [7]. The benefit of this approach is that the system is able to continuously monitor if there is any unauthorized access that occurs.

Meanwhile, static authentication approach collect data from the user and verify their access and privileges in manipulating the data, for example, at the login time [7]. This accessing service will be valid until the user logs out from the session. The combination of username and password is a

popular method for static authentication. Nevertheless, there is a drawback for static authentication in which this approach will authenticate the user only at the beginning of each session. The system will remain unnoticeable if there is any change of user in case of attacks [6].

In this paper, we survey the most recent advancement in biometric authentication system. However, our focuses are only on behavioral-based biometric authentication. In order to evaluate the accuracy of behavioral-based biometric authentication [8], there are three common measurements which are false rejection rate (FRR), the percentage of users' wrongly denied access to a system; false acceptance rate (FAR), the percentage of users wrongly authorized by a system; and equal error rate (EER), the value of the FRR and FAR when a system is tuned to have an equal FAR and FRR. Generally, in order for the authentication system to be more practical, it must have the following features that are accuracy, quick response, and difficult to be forged [9].

The remainder of this article is organized as follows: Section 2 discusses the biometric authentication. The subtopic in this section described the taxonomy of user authentication methods in each category emphasizing on their advantages and disadvantages. The description of behavioral-based biometric authentication system for every paper is discussed in details. Section 3 presented a discussion and future research direction in the development of behavioral-based biometric authentication system. Finally, Section 4 concludes the paper.

2. Authentication

2.1. User authentication methods

The most important key for the authentication process is the uniqueness of security measures, which in general can be categorized into something a user knows (password), something a user has (smart card), or something a user is (biometrics) [10–13]. Some examples of knowledge-based method, possession-based method, and biometric-based method can be found in **Figure 1**.

2.1.1. Knowledge-based method

Knowledge-based technique is commonly used to secure the access for systems [14]. The two famous examples are the pin and password. The password is normally entered at the beginning of any communication or operation which is only allowed if user has the correct one. The benefits for using conventional password are no specialized personnel required, simple, easy to use, and easy to remember. Unfortunately, passwords have many problems in that it is highly vulnerable to brute force attacks, password guessing, and key-loggers. The drawback is that once the password is compromised, an opponent can easily exploit a victim's account [15].

The marbles gap approach which comprises of password in a form of arbitrary sequence of marbles during authentication process can be found in [16]. The user needs to drag the digits in the right direction into the center of the screen. After that, it immediately reappears on the prior position. In order to leave smudge traces, three graphic-based authentication methods were implemented, which are one grid-based and two randomized graphical approaches.

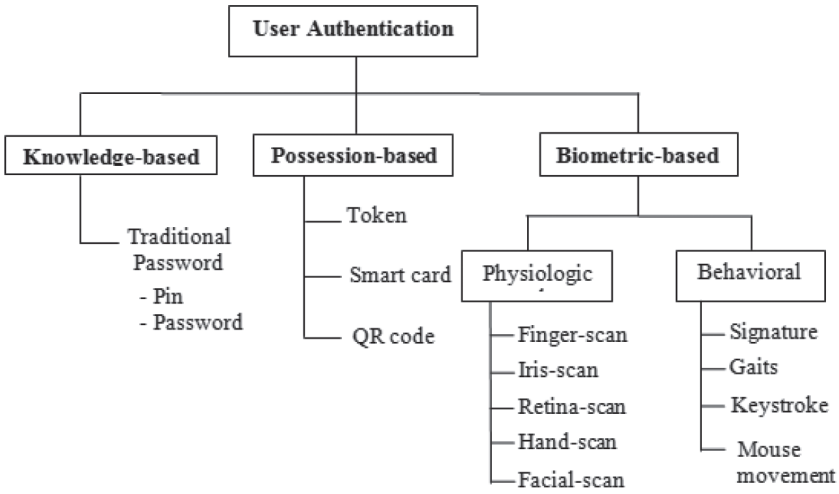

Figure 1. Taxonomy of user authentication methods.

Another authentication scheme for smartphone was established by using the matrix values of image [17]. This approach requires synchronization in advance between the smartphone and the service server. For the task of authentication, the user must react to the service server by inputting an existing combination of text-based and graphic-based passwords and thus providing better accuracy.

Ref. [18] proposed a location-based authentication approach using smartphone. The static (captured at login session) and continuous (captured during the session) location information were used. The two different locations of APIs were utilized during location verification. The location was verified and compared prior deciding whether the user is valid or not. This system can provoke errors during verification process caused by overlapping in location. Therefore, the security of the system introduced depends on the effectiveness of location verification.

Ref. [19] presented the physical proximity to guarantee security using a modulated illumination of smartphone screens to transmit PIN. The user enters a PIN on smartphone. By using a cheap bespoke receiver unit, the PIN is transmitted via temporary patterns of light on the screen. This approach was the right choice to ensure confidentiality against man-in-the-middle attacks.

The hybrid graphical password approach which is the mixture of recall and recognition-based schemes provided more secure system according to the use of graphical and textual password [20]. During registration phase, the user selects a username and a textual password and then chooses an object as password by drawing. All the information is stored in a database. During the authentication process, the user enters username and textual password and then draws the pre-selected objects. As expected, this scheme is not intended for users without drawing capability.

Table 1 shows a summary of various existing user authentication schemes that falls under knowledge-based category listed with advantages and disadvantages. Due to these advantages, the area of knowledge-based method for user authentication becomes less unpopular for exploration by the researchers.

Author	Knowledge	Approach	Advantages	Disadvantages
[16]	Graphical password	The marbles authentication method	This method has no upper restriction for the password space	The pattern of key arrangement must be recognized by the user
[17]	Graphical password	Matrix values of image	Provides more accuracy caused by the combination of sensors	Power consumption
[18]	Location	Location-based authentication	• Used the mobile function • Easy to use	Can provoke errors in verification caused by the overlapping in location
[19]	PIN	A modulated illumination of mobile device screens to transmit PIN	Assures confidentiality against attacks	Light sensor works within limited geographic scope
[20]	Graphical password	Recall and recognition-based schemes	More secure caused by the combination of graphical and textual password	Can provoke login error if the user does not have drawing capability

Table 1. Summary of knowledge-based method.

2.1.2. Possession-based method

The usages of traditional password have already been indicated as not sufficiently secure and inconvenient as a security measure. The possession-based method was proven to eradicate the risk of an attacker to guess passwords and is predicted to raise the level of security to data. This method makes use of things the user personally possesses such as token, smart card, and QR code.

Any objects or devices that can be used during authentication process are called hardware tokens. They are available in various forms such as a mobile device [21] or an easy-access device (key fobs and smartphones). The smart card reader (NFC-enabled smartphones) approach has been introduced with the combination of PIN and smart card [22]. The PIN is managed as a temporary PIN. The use of temporary PIN reduces the chance for an attacker to distinguish the permanent PIN.

The user authentication using QR code identification approach was implemented in this system [23]. During verification phase, the user makes a request from the server; in return, the server will extract the information about that user. The benefit of this approach is that it is known to be faster than the certificate system.

A summary of possession-based category is shown in **Table 2**. Possession-based methods are proven to eradicate the risk of an attacker to guess passwords easily from knowledge-based method. Since the token is needed to be present during the authentication process, the drawbacks of physical token are that, from the stolen or lost token, an attacker might gain an authorized access. Thus, the possession-based method for user authentication can still be considered as weak.

2.1.3. Biometric-based method

The use of human characteristics is the best solution compared to the user that personally knows and possesses [14]. In other words, biometric-based method cannot be forgotten or lost

Author	Possesses	Approach	Advantages	Disadvantages
[22]	PIN + smart card	Smart card reader (NFC-enabled smartphones)	The use of a temporary pin will reduce the chance for an attacker to detect the permanent pin	Public terminal or computer is required as an input and output device for smart cards
[21]	• Acoustic token • Magnetic token	Sound waves and static magnetic fields	Less prone to snooping	A sharp drop in the strength of the magnetic field formed can cause complications to the user
[23]	QR code	QR code identifying for user authentication	• Easy to use • Low cost • Reduces the memorization of human	—

Table 2. Summary of possession-based method.

in contrast to token, smart card, and password [24]. A biometric system is basically a pattern recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses or exhibits [25]. These authentication methods identify the user as themselves based on measurable physiological or behavioral characteristics.

2.1.3.1. Physical biometrics

Various technologies of physiological biometrics including finger scan, iris scan, retina scan, hand scan, and facial scan have been proposed and developed using measurements from the human body. There was evidence that the best accuracy can be obtained by using the physical biometric-based method. **Table 3** shows a summary of biometric-based method (physical biometric) for user authentication.

Fingerprint is the most famous features in biometric-based method and has shown to exhibit the best performance among others. Some of the approaches under fingerprint are of edge-based approach [26] and the rule mining approach [27], as well as the technique of image preprocessing region segmentation [28]. The advantages of using fingerprint are the ease of use and high in authentication accuracy. Nowadays, the fingerprint scanner is used widely among the user.

The concept of facial recognition technique through a vertical pose recovery fast semi-3D face [29] and fragile watermarking based on chaos theory [30] provided an impressive accuracy rate. Moreover, an extra security measure is achievable with the combination of this technique and other user authentication methods such as PIN.

Ref. [31] introduced a Daubechies wavelet transform approach to increase the performance rate for iris recognition. The iris is found to be the most accurate feature and being neither duplicable. Even so, when there are obstacles during the scanning process, the decision on recognition may be disrupted.

2.1.3.2. Behavioral biometric

The other group of biometric-based method is the behavioral biometrics, where users are identified based on their human actions such as signature, gaits (the way humans walk), keystroke dynamics (typing styles), and mouse dynamics [32].

Author	Recognition	Approach	Advantages	Disadvantages
[26]	Finger scan	Edge-based approach	Ease of use	Sensitive to camera limitations
[27]	Finger scan	Rule mining	Good in case of phone loss	Bad performance
[28]	Finger scan	Image preprocessing region segmentation	Ease of use	The higher templates that save in enrollment database, the execution time for the verification increases
[29]	Facial scan	Vertical pose recovery Fast semi-3D face	Extra security caused by combining with PIN	High energy consumption
[30]	Facial scan	Fragile watermarking based on chaos theory	Fast speed of authentication process	Not completely secured compared to other techniques
[31]	Iris scan	Daubechies wavelet transform	Increase the recognition of performance rate	Time- and energy-consuming

Table 3. Summary of biometric-based method (physical biometric).

Author	Recognition	Approach	Advantages	Disadvantages
[33]	Gaits	Linear regression classifier (KNN)	Biometric-based authentication with the same efficiency	Depends on the ideal conditions that the owner holds and operates the device in the same style all the time
[34]	Gaits	Classifier (KNN)	Do not involve explicit user interaction during verification process	Requires the punctual calibration of accelerator
[36]	Keystroke dynamics	SVM	Quick and easy configuration of individual thresholds without impostors' data	Large number of data required
[37]	Keystroke dynamics	SVM	The cheapest and easiest for the implementation process	Wasting of time for the user during enrollment process
[38]	Keystroke dynamics	Random forest	• Low cost • Replaceable in the event of compromise	Not sufficient for a high-security environment
[40]	Signature	Fuzzy	Well established for automatic signature verification	—
[39]	Signature	SVM	—	• Limited number of samples to be used for learning • The ability of the system to discriminate the forgeries

Table 4. Summary of biometric-based method (behavioral biometric).

In general, the direction of movement is detected by the magnetometer, while the gait recognition is detected by the gyroscopic sensor and accelerometer [33, 34]. For verification purposes, these authors used the same classifier, which is the K-nearest neighbor (K-NN). The gait recognition has a similar efficiency to the other biometric-based authentication. Nevertheless, the user is required to walk for a certain distance before the process of verification can occur.

Keystroke dynamics is one of the automated methods for verifying the identity of the user based on the manner and rhythm of typing on the keyboard [35]. In paper [36, 37], the authors used the support vector machine (SVM) as a classifier for the development of the system. Another approach that is usually used for the implementation of keystroke dynamics is random forest which can be found in [38].

Signature recognition is another user authentication scheme that works by analyzing handwriting style, in particular the signature. In the offline signature verification, [39] introduced the support vector machine (SVM) classifier, while [40] proposed fuzzy modeling based on the Takagi-Sugeno (TS) model. **Table 4** shows a summary of biometric-based method (behavioral biometric) for user authentication.

3. Behavioral-based biometric authentication

This section aims to find the good techniques for behavioral-based biometric authentication. **Figure 2** shows the various machine learning techniques that can generally be categorized into supervised (classification) and unsupervised (clustering).

Supervised machine learning can be used to classify the data much more accurately. In literatures, researchers have used classification techniques such as K-nearest neighbor (K-NN) [41], multilayer perceptron (MLP) [42], dynamic time warping (DTW) [43], neural network [7, 5, 44], decision tree algorithm [45], normalization and leave-one-out method [46], and support vector machine (SVM) [9, 47, 48]. These techniques have improved the performance of the system, and the results have shown some significant achievements in their respective domains. Meanwhile, unsupervised machine learning can be used to perform data reduction task by filtering out unrepresentative data. The data which will not be able to cluster correctly can be considered as outlier's data. After the reduction task, the classification result is expected to achieve optimal solution. The clustering algorithm can be further subcategorized into flat/partitioning-based and hierarchical-based clustering algorithm [49, 50].

The essential objective for the implementation of the behavioral-based biometric authentication is to acquire the accuracy and also to improve the performance of the system. This goal leads to the creation of a great classifier technique to solve the accuracy problems related to biometric authentication.

Ref. [47] developed an android application using touch-swipe biometric approach. In this work, touchscreen and motion data were collected through a physiological questionnaire. Parameters that are measured were duration, average velocity, mean X, mean Y, mean Z,

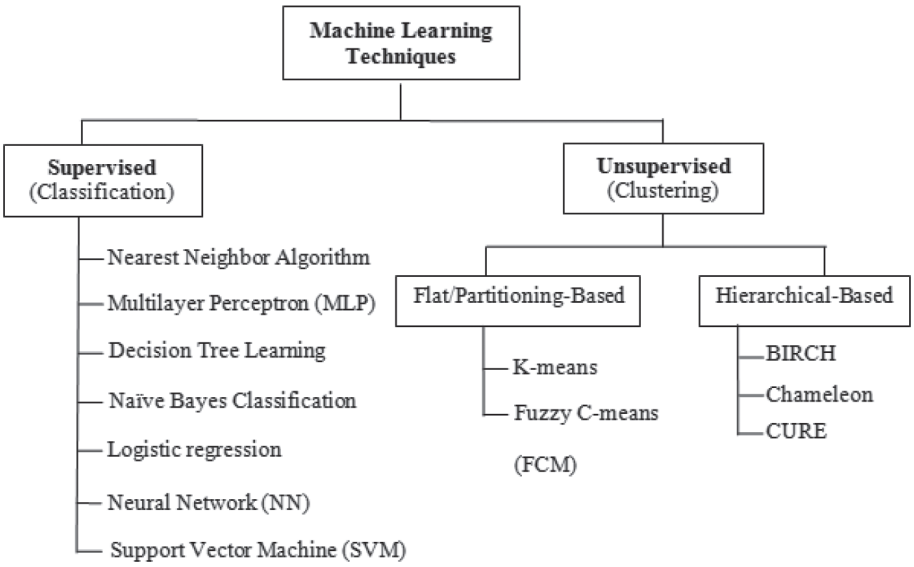

Figure 2. Classification of machine learning techniques.

length of trajectory, acceleration at start, midstrok pressure, midstrok finger area, mean pressure, and mean finger area. The author used support vector machine (SVM) as a classifier, and data analysis was done using WEKA software tool. The result in authentication of equal error rate (EER) was improved from single swipe (4%) to five swipes (0.2%).

Ref. [48] implemented a simple and efficient dynamic user authentication method. Authors also developed the data collection software that runs as the background job and without affecting other applications. This software has extracted the features such as click elapsed time, movement speed, movement acceleration, and relative position of extreme speed and used support vector machine (SVM) technique for classification of the data. This approach achieved the acceptable level of performance with false acceptance rate (FAR) of 0.37% and false rejection rate (FRR) of 1.12%.

Ref. [9] introduced a verification system based on mouse movements using logging tool recording user input (RUI). This system is able to verify a user accurately using newly defined angle-based metrics such as direction, angle of curvature, and curvature distance. This paper used support vector machine (SVM) on the design of the classifier user verification process. Around 30 users participated in this experiment. During their routine computing activities, the mouse movement data were recorded continuously. The result in an EER was recorded at 1.3%.

Ref. [51] used a mouse dynamic dataset from ISOT research lab (University of Victoria). This paper has applied Learning Algorithm for Multivariate Data Analysis (LAMDA) for data analysis. The evaluation of accuracy using 48 users achieved a FAR of 0% and a FRR of 0.36%.

Ref. [6] presented a static approach in which the user needs to perform a task called "follow the maze." Then, mouse movements are recorded to compute the velocity for X and Y

directions. In the verification phase, edit distance (also called Levenshtein distance or dynamic time warping) is used for the purpose of comparison between training and testing dataset. Experiment was conducted involving 28 participants including people highly skilled in computer and people not so skillful in using a mouse device. Nevertheless, they are set to use the same mouse device during the experiment. The result for EER was measured at around 27%.

Ref. [5] presented a continuous user authentication approach with higher-level actions, and the characteristics recorded are distance, action type, direction, and duration. The parameters that are involved in this research were movement speed, direction of movement, type of action, traveled distance, and movement elapsed time. The main experiment involved 22 participants, and 284 hours of raw data are collected over 998 sessions. This paper has applied artificial neural network for the classification of data. The result was presented using receiver operating characteristic (ROC) curves and a confusion matrix yield at the crossover point. This approach achieved the accuracy with FAR of 2.4649% and FRR of 2.4614%.

Ref. [52] proposed a static authentication which presented an enrollment by moving the mouse toward the dots drawn sequentially on the screen. Besides, the user's mouse movements were computed to generate features for enrolment signature. During verification process, the user follows the dots pattern identical to that of an enrolment phase. Then, this value was compared with the enrollment signature. This experiment involved 15 users, and they must use the same computer and mouse. The equal error rate (EER) for this system was recorded at 15%.

Ref. [45] presented a system that is related to the continuous approach in which raw mouse data was preprocessed to build a model of a user's behavior. The raw features such as speed, distance, frequency, and angle were extracted to compute the mean, standard deviation, and third-moment values for N data points. This paper has applied a supervised learning method, a decision tree algorithm for classification. This algorithm provides an intelligible representation to discriminate among K users for decision-making process. An authentication experiment was participated by 11 users. They were instructed to run Internet Explorer using their own personal computer. The result achieved for an average false acceptance rate (FAR) was 0.43%, and an average false rejection rate (FRR) was 1.75%.

Ref. [44] introduced an approach for providing secure access over the Internet using biometric authentication. The system used a hybrid approach, which was the combination of keyboard and signature to ensure that the set of credentials supplied to the system at the login stage is genuine. In this experiment, the author developed a web-based applet for the collection of data. For keyboard, the parameters that involved were latency times and hold times, while for signature, the parameters used were angle and distance. This paper was applied in neural network for data analysis. The evaluation of accuracy achieved a FAR of 4.4% and a FRR of 0.2%.

Table 5 shows a list of recent works on different behavioral-based biometric authentication approach that includes the collection of data, the parameter measured, the data analysis, the software used, and the measurement of accuracy. The false rejection rate (FRR), false acceptance rate (FAR), and equal error rate (EER) for every approach are also investigated. Briefly, many

Author	Biometric approach	Data collection	Parameter (feature extraction)	Data analysis (classifier)	Software used	Measurement of accuracy
[47]	Touch swipes	Android (psychological questionnaire)	**Raw data:** touch action; X and Y coordinate; X, Y, and Z gravity; pressure exerted; and finger area **Feature vector:** duration, length of trajectory, average velocity, acceleration at start, midstrok pressure, midstrok finger area, mean pressure, mean finger area, mean X, mean Y, and mean Z	SVM	WEKA	EER
[48]	Mouse dynamics	Data collection software	**Feature vector:** click elapsed time, movement speed, movement acceleration, and relative position of extreme speed	SVM	Pattern-growth-based mining method	FAR, FRR
[9]	Mouse movement	Recording user input (RUI)	**Raw data: action type**, time stamp, coordinate X, and coordinate Y **Feature vector:** three fine-grained angle-based metrics (direction, angle of curvature, and curvature distance)	SVM	—	EER
[51]	Mouse dynamics	ISOT mouse dataset	Movement speed, direction of movement, type of action, traveled distance, and movement elapsed time	Learning Algorithm for Multivariate Data Analysis (LAMDA)	MATLAB	FAR, FRR
[6]	Mouse dynamics	GUI	**Feature vector:** horizontal and vertical track velocity	Edit distance metrics	—	EER
[5]	Mouse dynamics	The client software	**Feature vector:** movement speed, direction of movement, type of action, traveled distance, and movement elapsed time	Neural network	MATLAB	FAR, FRR
[52]	Mouse movement	GUI	**Feature vector:** speed, deviation, positive angle, and negative angle (average, SD, minimum, maximum)	Comparing value with the range of the user's counter value (exact value)	—	EER
[45]	Mouse dynamics	Mouse dynamic application	**Raw data:** speed, distance, frequency, and angle **Feature vector:** mean, standard deviation, and third-moment values for N data points	Decision tree algorithm	—	FAR, FRR

Author	Biometric approach	Data collection	Parameter (feature extraction)	Data analysis (classifier)	Software used	Measurement of accuracy
[44]	Hybrid approach (keyboard + signature)	Web-based applet	**Keyboard:** latency times and hold times **Signature:** angle and distance (two approaches used to extract—ranking approach and genetic approach)	Neural network	—	FAR, FRR

Table 5. Comparison of related works for behavioral-based biometric authentication.

classifier techniques have been developed in biometric authentication fields such as neural network, decision tree algorithm, Learning Algorithm for Multivariate Data Analysis (LAMDA), and SVM. However, there is still room to enhance the accuracy of FAR and FRR in this field.

4. Discussion

Nowadays, the knowledge-based methods are commonly used because they are simple, economic, and convenient mechanisms to be used and implemented. However, these methods are also known as being an extremely poor form of protection. There are several ways in which an impostor can attack password-protected systems. The most common form of attack is password guessing. Authentication can also use something that user has as alternatives such as tokens, smart card, and QR code. However, these approaches does not lend itself particularly well in the above situation either. These kinds of approaches are more secure to use than a user's PIN or password. Thus, this possession-based method for user authentication can be considered weaker still. To overcome the drawbacks of those authentication methods, research has been shifted into biometric-based methods for the purposes of authentication, as biometric characteristics are not possible for sharing and repudiating due to uniqueness. Behavioral biometrics is the field of study related to the measure of uniquely identifying measurable patterns in human activities. The term contrasts with physical *biometrics*, which involves innate human characteristics such as fingerprints or iris patterns. **Table 6** shows the user authentication method that can be generally categorized into four categories.

Method	Instances	Properties
Something the user knows	PIN, password, etc.	Can be shared and forgotten
Something the user has	Token, smart card, QR code, etc.	Can be lost and duplicated
Something the user is	Finger scan, iris scan, retina scan, hand scan, facial scan, etc.	Not possible to share and repudiate
Something the user exhibits	Signature, gaits (the way humans walk), keystroke dynamics (typing styles), mouse dynamics, etc.	Not possible to share and repudiate

Table 6. Methodologies of user authentication.

In reality, many behavioral-based biometric methods have been proposed. However, the implementation and deployment are still lacking due to a few reasons such as costly devices, difficult to implement, and sometimes lack of accuracy.

5. Conclusion

This survey provides a comprehensive study on machine learning techniques in the domain of behavioral-based biometric authentication. Particularly, we reassess papers published between the years 2003 and 2016. First, we introduce the concept of biometric authentication and its application. Second, we present the taxonomy of authentication methods with detailed discussion on knowledge-based, possession-based, and biometrics-based methods. In the section of behavioral-based biometric authentication, we discuss the two subcategories of machine learning techniques which are supervised (classification) and unsupervised (clustering) techniques. We investigate each subcategory that has been implemented in the previous behavioral-based biometric authentication. In the end of this paper, we should be able to acquire relevant knowledge required for enhancing the performance of the behavioral-based biometric authentication.

Acknowledgements

This research was supported by the Malaysian Ministry of Higher Education [Grant No. FRGS/1/2017/ICT03/UNISZA/02/1 (RR228)].

Conflict of interest

All authors agreed that there is no conflict of interests.

Author details

Nurul Afnan Mahadi, Mohamad Afendee Mohamed*, Amirul Ihsan Mohamad, Mokhairi Makhtar, Mohd Fadzil Abdul Kadir and Mustafa Mamat

*Address all correspondence to: mafendee@unisza.edu.my

Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut, Malaysia

References

[1] Kissel R. Glossary of Key Information Security Terms. Maryland: National Institute of Standards and Technology; 2013. DOI: 10.6028/NIST.IR.7298r2

[2] Stapleton JJ. Security without Obscurity: A Guide to Confidentiality, Authentication, and Integrity. Boca Raton: CRC Press; 2014

[3] Clarke N. Transparent User Authentication: Biometrics, RFID and Behavioural Profiling. London: Springer Science & Business Media; 2011

[4] CNSS. Committee on National Security Systems (CNSS). Glossary, CNSSI No. 4009. April 6, 2015. Available from: https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf

[5] Ahmed AAE, Traore I. A new biometric technology based on mouse dynamics. IEEE Transactions on Dependable and Secure Computing. 2007;**4**(3):165-179

[6] Bours P, Fullu CJ. A login system using mouse dynamics. In: IIH-MSP 2009-2009 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing; 2009, pp. 1072-1077

[7] Jorgensen Z, Yu T. On mouse dynamics as a behavioral biometric for authentication. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security– ASIACCS '11; 2011. pp. 476

[8] Gorodnichy DO. Evolution and evaluation of biometric systems. In: Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009) Evolution, (Cisda); 2009

[9] Zheng N, Paloski A, Wang, H. An efficient user verification system via mouse movements. In: Proceedings of the 18th ACM Conference on Computer and Communications Security; 2011. pp. 139-150

[10] Vongsingthong S, Boonkrong S. A survey on smartphone authentication. Walailak Journal of Science and Technology. 2015;**12**(1):1-19

[11] Sahu SB, Singh A. Survey on various techniques of user authentication and graphical password. International Journal of Computer Trends and Technology (IJCTT). 2014; **16**(3):98-102

[12] Bhanushali A, Mange B, Vyas H, Bhanushali H, Bhogle P. Comparison of graphical password authentication techniques. International Journal of Computer Applications. 2015;**116**(1):975-8887

[13] Rittenhouse RG, Chaudhry JA. A survey of alternative authentication methods. In: International Conference on Recent Advances in Computer Systems, (Racs 2015); 2015. pp. 218-220

[14] Saifan R, Salem A, Zaidan D, Swidan A. A survey of behavioral authentication using keystroke dynamics: Touch screens and mobile devices. Journal of Social Sciences. 2016;**55**(11):29-41

[15] Jesudoss A, Subramaniam NP. A survey on authentication attacks and countermeasures. Indian Journal of Computer Science and Engineering (IJCSE). 2014;**5**(2):71-77

[16] Von Zezschwitz E, Koslow A, De Luca A, Hussmann H. Making graphic-based authentication secure against smudge attacks. In: Proceedings of the 2013 International Conference on Intelligent User Interfaces–IUI '13; 2013. pp. 277

[17] Kim H, Lee K, Jung, Y. A design of authentication strengthening scheme using matrix values of image in smart phone environment. In: Proceedings of the 1st International Conference on Convergence and It's Application, 24; 2013. pp. 179-182

[18] Takamizawa H, Tanaka N. Authentication system using location information on ipad or smartphone. International Journal of Computer Theory and Engineering. 2012;**4**(2):153-157

[19] Nickel C. Accelerometer-Based Biometric Gait Recognition for Authentication on Smartphones [Doctoral dissertation]. Technische Universität; 2012

[20] Khan WZ, Aalsalem MY, Xiang Y. A graphical password based system for small mobile devices. IJCSI International Journal of Computer Science Issues. 2011;**8**(5):145-154

[21] Bojinov H, Boneh D. Mobile Token-based authentication on a budget. In: Proceedings of the 12th Workshop on Mobile Computing Systems and Applications - HotMobile '11; 2011. pp. 14

[22] Ghogare SD, Jadhav SP, Chadha AR, Patil HC. Location based authentication: A new approach towards providing security. International Journal of Scientific and Research Publications. 2012;**2**(1):2250-3153

[23] Bianchi A, Oakley I, Kwon DS. Using mobile device screens for authentication. In: Proceedings of the 23rd Australian Computer-Human interaction conference, OzCHI 2011; 2011. pp. 50-53

[24] Lakshmi P, Susan V. Biometric authentication using ElGamal cryptosystem and DNA sequence. International Journal of Engineering Science and Technology. 2010; **2**(6):1993-1996

[25] Prabhakar S, Pankanti S, Jain AK. Biometric recognition: Security and privacy concerns. IEEE Security & Privacy Magazine. 2003;**1**(2):33-42

[26] Stein C, Nickel C, Busch C. Fingerphoto recognition with smartphone cameras. In: Proceedings of the International Conference of the Biometrics Special Interst Group; 2012. pp. 1-12

[27] Gupta P, Wee TK, Ramasubbu N, Lo D, Gao D, Balan RK. HuMan: Creating memorable fingerprints of mobile users. In: IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2012, (March); 2012. pp. 479-482

[28] Cheng K, Kumar A. contactless finger knuckle identification using smartphones. In: Proceedings of the International Conference of the Biometrics Special Interest Group 2012; 2012. pp. 1-6

[29] Hu JY, Sueng CC, Liao WH, Ho CC. Android-based mobile payment service protected by 3-factor authentication and virtual private Ad Hoc Networking. In: 2012 Computing, Communications and Applications Conference (ComComAp 2012); 2012. Vol. 1. pp. 111-116

[30] Hernandez CP, Torres-Huitzil C. A fragile watermarking scheme for image authentication in mobile devices. In: Electrical Engineering Computing Science and Automatic Control (CCE), 2011 8th International Conference on (pp. 1-6). IEEE; 2011. pp. 39-43

[31] Somnath D, Samanta D. Improved feature processing for iris biometric authentication system. International Journal of Computer Systems Science and Engineering (IJCSSE), World Academy of Science. 2010;**4**(3):455-462

[32] Babich A. Biometric authentication. Types of Biometric Identifiers. 2012:1-56

[33] Lin C, Liang D, Chang CC, Yang CH. A new non-intrusive authentication method based on the orientation sensor for smartphone users. In: 2012 IEEE Sixth International Conference on Software Security and Reliability; 2012. pp. 245-252

[34] Nickel C, Wirtl T, Busch, C. Authentication of smartphone users based on the way they walk using k-NN algorithm. In: 2012 Eighth IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP); 2012. pp. 16-20

[35] Shen P, Jin A, Tee C, Song T. Expert systems with applications keystroke dynamics in password authentication enhancement. Expert Systems with Applications. 2010; **37**(12):8618-8627

[36] Giot R, El-abed M, Hemery B, Rosenberger C. Unconstrained keystroke dynamics authentication with shared secret. Computers and Security. 2011;**30**(6-7):427-445

[37] Giot R, El-Abed M, Rosenberger, C. Keystroke dynamics authentication for collaborative systems. In: 2009 International Symposium on Collaborative Technologies and Systems, CTS 2009; 2009. pp. 172-179. https://doi.org/10.1109/CTS.2009.5067478

[38] Bartlow N, Cukic B. Evaluating the reliability of credential hardening through keystroke dynamics. In: IEEE 17th International Symposium in Software Reliability Engineering, 2006. (ISSRE'06); 2006. pp. 117-126

[39] Justino EJR, Bortolozzi F, Sabourin R. A comparison of SVM and HMM classifiers in the off-line signature verification. Pattern Recognition Letters. 2005;**26**:1377-1385

[40] Hanmandlu M, Hafizuddin M, Yusof M, Krishna V. Off-line signature verification and forgery detection using fuzzy modeling. Pattern Recognition. 2005;**38**:341-356

[41] Ajufor N, Amalraj A, Diaz R, Islam M, Lampe M. Refinement of a mouse movement biometric system. In: Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 2nd, 2008; 2008, pp. 1-8

[42] Buriro A, Crispo B, Delfrari F, Wrona K. Hold & Sign: A novel behavioral biometrics for smartphone user authentication Hold & Sign: A novel behavioral biometrics for smartphone user authentication. In: IEEE Security and Privacy Workshops MoST 2016, (MAY); 2016

[43] Xiao G, Milanova M, Xie M. Secure behavioral biometric authentication with leap motion. In: 4th International Symposium on Digital Forensics and Security, ISDFS 2016– Proceeding; 2016. pp. 112-118

[44] Everitt RAJ, McOwan PW. Java-based internet biometric authentication system. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2003;**25**(9):1166-1172

[45] Pusara M, Brodley CE. User re-authentication via mouse movements. In: Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security VizSECDMSEC 04; 2004. pp. 1-8

[46] Hamid NA, Safei S, Dhalila S, Satar M, Chuprat S, Ahmad R. Randomized mouse movement for behavioral biometric identification. International Journal of Interactive Digital Media. 2013;**1**(2):52-57

[47] Antal M, Szabó LZ. Biometric authentication based on touchscreen swipe patterns. Procedia Technology. 2016;**22**(October 2015):862-869

[48] Shen C, Cai Z, Guan X. Continuous authentication for mouse dynamics: A pattern-growth approach. In: Proceedings of the International Conference on Dependable Systems and Networks; 2012

[49] Fahad A, Alshatri N, Tari Z, Alamri A, Khalil I, Zomaya A, et al. A survey of clustering algorithms for big data: Taxonomy & empirical analysis. IEEE Transactions on Emerging Topics in Computing. 2014

[50] Berkhin P. A survey of clustering data mining. In: Grouping Multidimensional Data. Berlin Heidelberg: Springer; 2006. pp. 25-71

[51] Nakkabi Y, Traoré I, Ahmed AAE. Improving mouse dynamics biometric performance using variance reduction via extractors with separate features. IEEE Transactions on Systems, Man and Cybernetics. 2010;**40**(6):1345-1353

[52] Hashia S, Pollett C, Stamp M, Hall M, Jose S. On using mouse movements as a biometric. In: Proceeding in the International Conference on Computer Science and Its Applications; 2005. Vol. 1