Journal of Ambient Intelligence and Humanized Computing (2023) 14:339–360
https://doi.org/10.1007/s12652-021-03301-x

ORIGINAL RESEARCH

A broad review on non-intrusive active user authentication in biometrics

Princy Ann Thomas[1] · K. Preetha Mathew[2]

Received: 24 November 2020 / Accepted: 1 May 2021 / Published online: 4 June 2021

Abstract
Authentication is the process of keeping the user's personal information as confidential in digital applications. Moreover, the user authentication process in the digital platform is employed to verify the own users by some authentication methods like biometrics, voice recognition, and so on. Traditionally, a one-time login based credential verification method was utilized for user authentication. Recently, several new approaches were proposed to enhance the user authentication framework but those approaches have been found inconsistent during the authentication execution process. Hence, the main motive of this review article is to analyze the advantage and disadvantages of authentication systems such as voice recognition, keystroke, and mouse dynamics. These authentication models are evaluated in a continuous non-user authentication environment and their results have been presented in way of tabular and graphical representation. Also, the common merits and demerits of the discussed authentication systems are broadly explained discussion section. Henceforth, this study will help the researchers to adopt the best suitable method at each stage to build an authentication framework for non-intrusive active authentication.

Keywords User authentication · Keystroke dynamics · Mouse dynamics · Voice recognition · Biometric

1 Introduction

In the present decade, the uses of digital devices have been tremendously increased in common places (Kuppusamy 2019). Also, it is hard to find anyone who does not use a computer, a laptop, or an android phone (Teh et al. 2019). All of these devices are internet-enabled and providing web access round for regular users (Vittori 2019). In addition, the banking sector is an area that faces numerous challenges (Partila et al. 2020) in the security field like payment authorization and identity verification (Shirvanian et al. 2019). Hence, the primary steps in bank applications are developing the privacy module for user verification (Dobbie 2020). This allows the user to be relatively confident, so that an intruder is not allowed without checking access of each account (Messerman et al. 2011). Some of the traditional authentication systems are signature verification, identity card verification (Clarke et al. 2009), and photographic evidence for verification. Also, authentication documents like passports o visas, and so on (Furnell et al. 2008). There are three types of authentications that are presently in use (Cao et al. 2020). First is a statement given by a person or some trusted authority with personal contact. Here, the person or object able to test the authenticity of the object that is being verified (Clarke et al. 2002). Second is a comparison of similar attributes of the authenticated object, which is previously known to be true of that object (Alshehri et al. 2017). The third type allows for using documents such as trademarks or certifications that are issued by a trusted authenticating authority. The second type is useful only if the forgery of the attributes is not easily accomplished (Bernabe et al. 2020). In computer security, user authentication is meant to prove that the user is the one who he claims to be (Zheng et al. 2014).

The logon method is a type 1 authentication factor that tests something the user knows (Saevanee et al. 2015). Moreover, remembering the complex pass-phrases is

✉ Princy Ann Thomas
princy@gecidukki.ac.in

K. Preetha Mathew
preetha.mathew.k@gmail.com

[1] Computer Science and Engineering Department, Government Engineering College, Painavu, Idukki, Kerala 685603, India

[2] Computer Science and Engineering Department, Cochin University College of Engineering Kuttanad (CUCEK), Pulincunnu, Kerala 688504, India

difficult for computer users, so that an identify management system was introduced to retrieve the required content of each user (Sinigaglia et al. 2020). But in some cases, the phrase retrieving model based on the management system is vulnerable to malicious activities (Rodwell et al. 2007). Furthermore, a token like a debit card is type 2 authentication factor, which indicates, what a user has to be. Biometrics like iris scanner or voice recognition is categorized as type 3 authentication factor that represents user status. On the other hand, a verification system based on speaker voice is an advanced technique in biometrics fields (Clarke and Furnell 2007). Here, the verification module has functioned on the basis of voice features, the features include, sound and pronunciation of each individual. Also, unimodal-based continuous authentication frames rely on single information sources such as face profiling, touch gesture, and so on (Kim et al. 2007). In today's digital life scenario, the authentication based on biometric system is widely reliable because the usual authentication system like password (Lee and Yim 2020), security codes, key sensors, etc., are high expensive in cost and need more resources to process the function. To minimize the work complexity the system known as biometrics is organized (Jagadeesan and Hsiao 2009). To reduce the execution time of authentication system the most people can prefer the login process (Jorgensen and Yu 2011). But in this logion process, several limitations are listed as impractical verification times, uncontrolled environment variables, and authentication for remote access. To end these issues, the smart authentication frame is introduced like keystroke, mouse dynamics, voice recognition, and so on. In keystroke authentication process, the user is authenticated through the typing style. In mouse-based authentication, users are authenticated via mouse action. Also, a voice authentication system is executed based on user voice (Zheng et al. 2011).

Nowadays, humans' lifestyles and needs are digitalized so securing the privacy information is a significant task. Moreover, the user would switch on his/her computer and start using the device for their normal work (Shirvanian et al. 2019). The security software should be confirmed that he/she are the authenticated users have the access token to access the system. This kind of system would be considered as non-intrusive user authentication system. Also to make the smart verification model, keystrokes, voice biometric, and mouse dynamics are discussed in this review article. Here, the mouse dynamics paradigm is functioned based on recording the mouse actions and keystroke dynamics are functioned based on typing style of each individual. Subsequently, the function parameters of mouse dynamics, voice biometrics, and keystroke dynamics are analysed and comparison assessment is made in tabular and graphical representation.

2 Behavioural biometrics

Nonintrusive behavioural biometrics was utilized to provide security for the stored data in the computer system. It attempts to study the normal behaviour of authentic users on a system and then to identify abnormal behaviour from the normal behavioural pattern (Fourati et al. 2020). Behavioural biometrics capture the characteristic patterns of the user's input, navigation through interfaces, and regular use patterns on both input devices as well as applications to create a virtual fingerprint of authentic user behaviour (Lang and Haar 2020). Hence, the behavioural biometrics has been provided a wide range of merits over conventional biometric strategies (Kaur and Khanna 2020). In addition, the gathered behavioural data no need any specific hardware architecture. So it has diminished the cost complexity (Ferrag et al. 2020).

The different types of behavioural biometric systems are normally characterized as voice identification, signature authentication, mouse dynamics, keystroke dynamics, swipe patterns, graphical confirmation system, gait recognition, emotion recognition, lip movement detection, biometric, and bio-signals (Patro et al. 2020). These parameters are proficiently utilized in Electrocardiogram (ECG) (Kim et al. 2019) and Electroencephalogram (EEG) (Bidgoly et al. 2020). The most recent research in each of these types has emphasized and shown greater potential for non-intrusive and continuous or active user authentication. The wide degree-based reliable security in biometric technology can obtain a huge rate of potential measure to verify each user. Moreover, behavioural biometrics is functioned based on the body actions of each individual. Hence, the body actions include fingerprint, lip movement, voice, and eye movement. Biometric authentication has many important applications especially in light of the current Covid-19 crisis like e-learning (Baró et al. 2020), digital banking, remote device access in IoT, and many more.

2.1 Voice biometric recognition

Voice biometric recognition leverages the unique features of the human voice to identify and authenticate an own user as shown in Fig. 1. The voice recognition system has a training phase and a recognition phase. During training, the system learns the characteristic traits of the user are enrolled. Later in the recognition phase, the system simply captures the user voice features and the audio recognition system compares it with the enrolled voice metrics. If a match occurs then the user is authenticated, else user is rejected by the verification system. Here, the chief significant score of voice- based biometric system is the

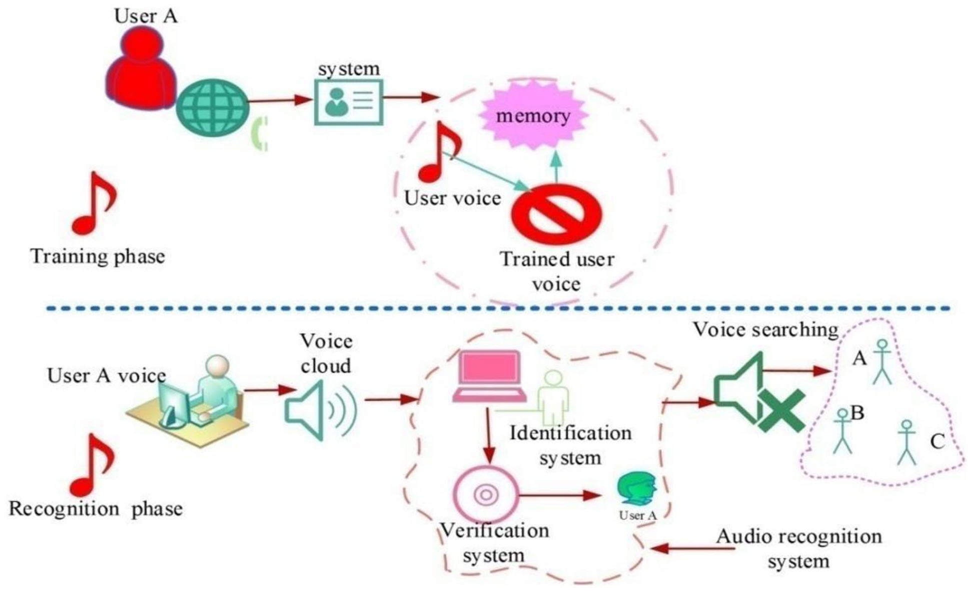


Fig. 1 Voice recognition system

speech by user is not recorded only it recognizes the sound to make the verification. The form of sound is produced based on the amount of air stream and obstructions in the way of airstreams like tongue, gums, and lips. Thus the high standard authentication strategy is appropriate for high-risk and security systems. Relatively, some applications need text analysis, because in some cases it is too difficult to beat an excellent profitable speaker authentication system by recording. Moreover, the input signal of voice is collected from telephone or microphone. Here, the telephone and microphone were placed very close to the mouth, thus the voice was differed based on each user. From the literature, it is concluded that voice biometric recognition normally operates in three ways namely text-dependent speaker confirmation, text prompted speaker authentication, and text-independent speaker verification. Moreover, the merits and limitations of voice biometrics are shown in Table 1.

Almaadeed et al. (2012) has discussed the speaker identification system that uses multimodal neural networks and wavelet analysis to authenticate the users. This system is a text-independent recognition system that uses a voting scheme for decision-making. Hence, the design improves the classical Mel-frequency Cepstral Coefficients (MFCC) as 15%, Equal Error Rate (EER) as 5%, accuracy 84 to 99%, and identification time as 40%. Moreover, the obtained results clearly revealed the performance of authentication process with the support of extracted features. The downside is that computational time is directly proportional to the number of features. Devising effective techniques to select features with the highest relevance would alleviate this problem to a certain extent. The joint speaker verification design was discussed by Sizov et al. (2015); it is another text-independent system that combines narrator verification and anti-spoofing by using an i-vector strategy for speaker modelling. The proficient score of the developed strategy is proven by incorporating the possible attacks.

Hence, the designed model has gained EER as 0.81% and 0.54% FAR for female voice. Moreover, this strategy has represented the speech by a high dimension vector incorporating background information to enhance the recognition system. The limitation behind in this model is the proposed replica is only developed for female voice datasets.

The computation complexity of i-vector methods can be reduced using dimensionality reduction (Medikonda et al. 2020). Even it has only achieved 15–30% accuracy under various simulated noisy conditions. Moreover, features extracted on different MFCC derivatives based on time series are analysed to improve the accuracy up to 98% using a Gaussian Mixture Model (GMM) for classification (Rakshit 2020). All of the above text-independent verification methods are usable with the non-intrusive active authentication process that satisfied user needs in the normal course of work.

Voice recognition systems are widely used in a part of access control systems for security. In addition, an access control system based on the EN 50133-1:1996 European standard (Galka et al. 2014) contains a voice authentication module that basically depends on text passwords. The system has utilized a modified background scheme called Gaussian Mixture and Hidden Markov Model for authentication process. Therefore, the proposed model has attained an EER rate of 3.4%. Navarro et al. (2015) has presented another interesting work on voice verification system. Here, the system hardware is enhanced with a vector floating-point unit in the microprocessor that increased the vector floating-point operation rapidity in the speaker verification algorithms. The modified architecture has yielded an EER of 7% under ideal conditions and yields 15% to 17% in adverse conditions. The downside of this method is in real-time environment the hardware needs modification to make the best results (Lin et al. 2013).

Voice biometric identification and authentication have been applied in many important applications especially user authentication on smart devices (Teh et al. 2019). Here, lip movement and voice authentication can work effectively even in noisy environments by using the already available device sensors (Vittori 2019). Intelligent voice bots [8] are a useful and cost-effective way to assure remote user authorization in digital banking (Partila et al. 2020). Moreover, voice has been combined with other biometric modalities to improve performance like EEG (Moreno-Rodriguez and Ramirez-Cortes 2020) with 90% accuracy. Also, other features are recorded that are swipe gestures, facial images with voice (Gupta et al. 2020). In several cases, the voice authentication model is designed using Gaussian membership with fuzzy vectors. Hence, the obtained exactness rate using this scheme is 95.45% (Abdul-Hassan and Hadi 2020).

Voice has also been investigated with voice mimicry attack (Vestman et al. 2020) and found to be vulnerable. Voice biometric security is normally tested against general datasets with less percentage of similar signature imposter data (Shirvanian et al. 2019; Sholokhov et al. 2020). The testing of ASV systems needs to incorporate the closest imposter model framework for more accurate results (Lakshmi et al. 2020) with the use of chaotic maps.

2.2 Authentication using keystroke dynamics

The keystroke dynamics paradigm is the study of keying rhythm of a user. Several studies have shown that experienced users have a specific typing pattern (Verwey 2019) that does not change much even with deliberate external stimuli. Hence, this makes the keystroke dynamics as very good candidate for a biometric signature. There is several comprehensive review works conducted on keystroke dynamics (Ali et al. 2017). Moreover, the keystroke process mostly depends on the timing of key presses and releases. The behaviour of keystroke for users may change depending on the layout of the keyboard (Rude 2019) and behavioural pattern of the user. So, it is seen that many of the distinctive behavioural patterns persist across different devices (Lipke-Perry et al. 2019) like a pianist who may have a distinct feel for a familiar instrument.

In addition, the keystroke dynamics are divided into fixed text or static text analysis and free text or dynamic text analysis. If there are different authentication processes then static approaches are utilized. Here, free text analysis of keystroke information was discussed, which allows continuous

Table 1 Merits and demerits of voice authentication system

Authors	Methods	Merits	Demerits
Almaadeed et al. (2012)	Decision based robust procedure	Here, the developed model has utilized the coefficients of mel-frequency to process the audio signal. Finally, the developed strategy has gained accuracy as 98.2%	If the dataset is complex then the developed frame model has gained high error rate and this leads to fall in accuracy rate Moreover, the key reason for achieving high error percentage is in this model the coefficients of linear function is not defined
Sizov et al. (2015)	Backend scheme	It has gained the finest accuracy rate with short duration	The chief limitation behind in this model is similar voice features were trained to verify the own users. Thus, the proposed system is not applicable in miss- match model
Medikonda et al. (2020)	Twofold dataset	The proposed scheme is evaluated under three diverse datasets and has diminished computational complexity and simulation time	But in some cases, it lacks in security because of high noise signal
Galka et al. (2014)	Embedded scheme	Here, the experimental works are done to validate the system reliability and function rate	However, the voice recognition model using micro processer paradigm is quite complicated task because of its memory size and processor components
Navarro et al. (2015)	Microprocessor- MicroBlaze in FPGA	The scheme required less period for voice recognition	In some circumstances, the gadget architecture needs some modifications and updates to perform voice verification system process. So, the FPGA frame needs more memory spaces to execute the function

or periodic authentication of a user. To incorporate varying behaviour of users over time, different machine learning approaches were studied to contribute the verification objective. As in voice and keystroke dynamics, several security threats were raised that tends to gain very less accuracy (Belman et al. 2020).

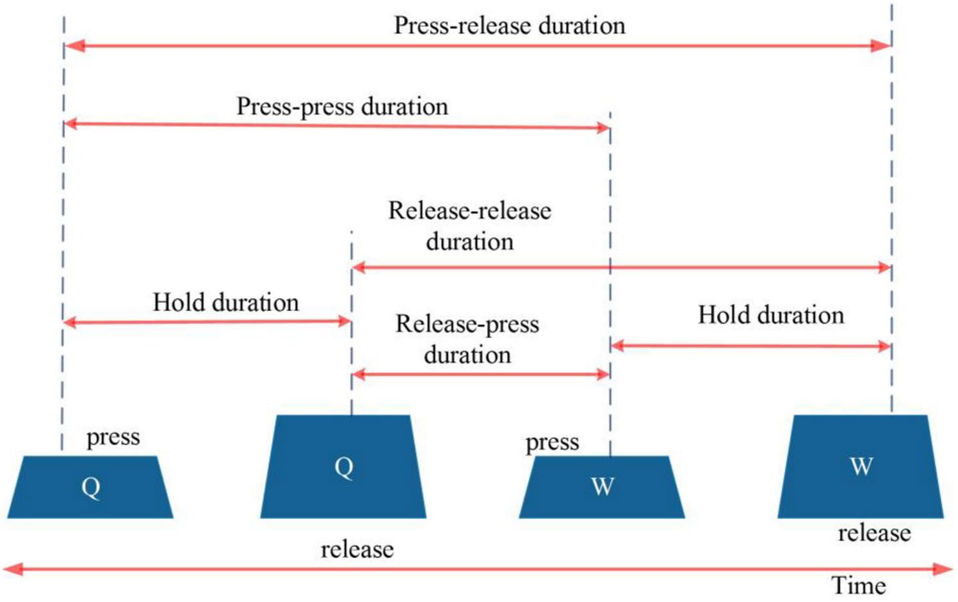
One of the pioneering works in the area of free script analysis was projected by Gunetti and Picardi (2005). The projected strategy has analyzed free text for authentication purposes using a custom interface in which the user is to type any text about 700–900 words. The typing rhythm is studied based on timing information of individual keystrokes and n-graph comparison of consecutive text entries. The process of keystroke function is elaborated in Fig. 2. The setup shows that the capture of keystroke data on a number pad is utilized to train the system. Once the training phase is complete the system is tested, where once again user keystroke dynamics is captured and matched against the user keystroke profile, which is stored during the training phase. If the user is authenticated then a prompt to type in a password is given. Another statistic method based on mutual feature vectors is used for authentication which was proposed by Wang et al. (2012). During the training phase, keystroke features of the authentic user are periodically generated and the events are stored in the database. Hereafter, while authenticating the keystroke of current users, previously saved feature vectors and distortion were calculated. Here experiments were conducted based on many passwords typed by the user. This work concentrates on short fixed texts, but the possibility of change in user behaviour with time is not taken into the consideration.

Chang et al. (2013) presented the hypothesize model, which states that the pause time intervals between different characters typing on the keyboard are caused since the user is unable to comprehend the spelling, unfamiliar words, and so on. Besides, the cognitive factor is unique for an individual. So, diverse ML is possible to apply in the authenticated system to verify the own users. Subsequently, by the analysis, the best results were reported for SVM as 0.055% FAR and 0.007% FRR. The set of experiments were conducted only on simulated environments thus its translation into real-time authentication is not clear. Moreover, the time required to train the system is not discussed. To overcome the problem of biometric permanence in biometric systems Pisani et al. (2015) proposed a timing phase system using keystroke dynamics authentication. Here the effect of change in a biometric signature over time is studied. Moreover, to estimate the time some adaptive biometric systems were utilized, which are usually worn to reduce intra-class variability with one-class classification algorithms.

Another interesting work on keystroke information by Kang and Cho (2015) made the important observation that current methods need to be customized for keyboards other than the traditional PC keyboard. Also, from the implementation, it is verified that authentication accuracy varies with the length of reference and test keystroke.

There are several application areas for this particular biometric method namely intrusion detection, which provides the solution for lost or forgotten password problems (Gunetti and Picardi 2005) in smartphones and other mobile devices (Gupta et al. 2020; Ali et al. 2019). Keystroke dynamics have

Fig. 2 Keystroke events



been used in the area of identifying user attitudes (Antal and Egyed-Zsigmond 2019) and confirming user demographics like age to prevent various cybercrimes. Finally, keystroke verification is less suitable for web-based applications since the mouse is used more frequently in this environment (Feher et al. 2012).

The summary of keystroke dynamics revealed that in all biometric systems hacking and loss of privacy could be at risk when a system is compromised. Keylogging is another disadvantage of this system, which can be alleviated using cryptography. The method is also vulnerable to replay attacks and spoofing. There is very little research in the area of security of keystroke dynamics. Keeping the captured data secure is the one-way solution for most issues and it needs to be studied in future.

2.3 Mouse dynamics

Mouse dynamics are similar to keystroke dynamics, the difference is that here the mouse movements and actions are used to regulate whether a user is reliable or not. Typically, mouse movements, gestures, clicks, and their timing information are collected in authentication systems based on mouse dynamics (Antal and Egyed-Zsigmond 2019). Just as in keystroke dynamics, the method has been used for both static authentication and active authentication with varied results. In static authentication, the mouse movement for a fixed task is collected during the training phase and a profile for the authentic user is created based on this fixed task. In the testing stage, the user once again performs the same task and the authentication system determines whether the user is authentic or an imposter. In an active user authentication, (Yıldırım and Anarım 2019) the task is not fixed and the scheme tries to authenticate the operator of a particular arrangement when he/she may be doing different tasks. Hence, the advantages and disadvantages of mouse dynamics are detailed in Table 2.

The training phase in this case would allow normal working without any restriction on the type of task or with limited restrictions. Consequently, during the testing phase, the system would try to match the profile created at the training phase and then determine how different the current user is from the registered user. Much of the existing work in mouse dynamics is on multimodal authentication systems but keystroke dynamics are most often clubbed with mouse dynamics. It is suggested that better performance may be attained when the mouse dynamics are clubbed with non-behavioural modalities like eye movement (Kasprowski and Harezlak 2018). Mouse dynamics have the potential to frame user authentication and to create adversarial mouse trajectories as same as characteristic features leveraged in authentication systems (Tan et al. 2019). Capturing the Temporal mouse information is captured for the authentication purpose, the commonly used mouse events are detailed in Table 3.

One of the initial works in mouse dynamics was done by Ahmed and Traore (2007), where Artificial Neural Networks (ANN) was designed to implement the authentication system. The experimental environment implements the passive authentication but allows users to select the desired operating environment and application. Moreover, the ANN was utilized to train the data and to build the signature of each user. It reported the FAR as 2.4649% and FRR as 2.4614%. Kenneth Revett et al. (2008) have been presented a graphical authentication system called mouse lock. It requires a user to select a group of images and move them along a particular direction in a particular sequence. The right combination is used as a password to authenticate the original user. The timing information of consecutive image movements are used to estimate if the operator or customer is authentic or not. The proposed strategy has achieved FAR and FRR rates between 0.02 and 0.05%. It would be much easier to identify a set of movements than the letters typed on a traditional password login. If the number of movements is increased drastically to avoid this then the actual login becomes a tedious process. Besides, this method is intrusive and unsuitable for continuous authentication. The first two columns indicate the type of mouse information captured; the next two are the mouse coordinates and the timing information in milliseconds.

The neural network with dimensionality reduction algorithms like PCA and ISOMAP plays a key role in the biometric system. So, Shen et al. (2009) made a study on behavioural variability of 10 long-term computer users with neural schemes. Finally, the designed model has reported an improved accuracy with dimensionality reduction by attaining the FAR as 0.055 and FRR as 0.03. The number of mouse clicks within the authentication frame is stated to be 20. The next logical question is whether it would be possible to identify an intruder effectively before a security breach is possible. For that, Feher et al. (2012) have been developed a new continuous authentication system that prioritized the mouse actions to reduce the execution time. A random forest classifier is built for each action type and a decision is made by combining the probabilities of each classifier. Hence, this work reports an EER rate as 0.1%. The time required for authentication is approximately 2 min. This method has the disadvantage of device dependant and non-inclusion of change in user behaviour with changing physical and mental surroundings that might affect the system performance. Ling et al. (2017) have been used mouse

Table 2 Advantages and disadvantages of mouse dynamics

Authors	Methods[a]	Advantages	Disadvantages
Antal and Egyed-Zsigmond (2019)	Performance assessment using Balabit data	All events of mouse scroll functions are recorded. Number of features extracted is 13. Positive result from test 411 and negative result from test 405	The process execution in short duration might cause dataset error, this tends to gain very less accuracy
Kasprowski and Harezlak (2018)	Eye moving and mouse dynamics frame	The projected scheme has gained better exactness measure and less error rate	Here, the eye statics are recorded in the less frequency; in that case, the designed scheme has obtained high flaw measure
Tan et al. (2019)	Balabit attack mitigation frame using neural network in mouse dynamics	By developing this scheme in mouse dynamics frame, the risk occurrence has reduced	It takes more time to execute the process. Also if the data is complex then wide range of flaw is recorded
Ahmed and Traore (2007)	Neural scheme configuration	Here, the designed neural network automatically predicts and records the mouse action events by its classification process. Thus it has gained good exactness measure	The drawback behind in this model is screen resolution because the signature is recorded in one range of resolution and the user detection is happened in other resolution. Thus it minimizes the accuracy measure. The next one is accelerator setting; the adjustment in rapidity settings can affect the system operation
Revett et al. (2008)	Graphical authentication procedure	Based on the key parameters the original users were detected. Hence the parameters are distance angle and speed	This system model detects the user by analysing the time of each user action. So only few attributes are applicable to carry this process. If the large size of dataset is trained then wide range of flaw measure is recorded
Shen et al. (2009)	Dimensional reduction	It was executed in short duration with high accuracy	Here, the investigation is made on 10 computer users' actions. So if the diverse dataset is trained then the detection performance might be diminished
Feher et al. (2012)	Random forest scheme	Simple to design the model, also wide range of accuracy improvement for verification is recorded	Diverse kind of mouse and mouse pads were diminished the system functions. Also, maximum time is needed to attain the finest point. On the other hand, the system contains maximum number of instances thus it has needed more memory space to run the execution
Lin et al. (2012)	Double frame classifier with regression model	In this scheme, the unwanted characters are removed in the initial layer of regression function. Hereafter, error mined data is entered into the classification layer to verify the original users	By the experimental evaluation, the projected scheme has obtained high false measure rate
Sayed et al. (2013)	Static authentication by neural scheme	The amount of data utilized for verification is 39 Testing samples 4, merits of this system is it has improved the identification measure. Here, the own users are recognized by their gestures	It has gained high flaw rate and less exactness measure. Moreover, the security aspects also questionable in this scheme
Ernsberger et al. (2017)	Mouse dynamics visualization system	This process is executed in short duration, verification process relatively very fast	Lacks in security against reply attack. Moreover, the system is operated in complex platform. Also, the developed framework is vulnerability for automated attacks
Cai et al. (2014)	Dimension reduction schemes	The matching variability has diminished by 76%. In all test cases, the process of feature space has gained better results	But identifying an appropriate feature space for real time application is a big threat in the mouse dynamics

Table 2 (continued)

Authors	Methods[a]	Advantages	Disadvantages
Hinbarji et al. (2015)	Back propagation based neural scheme	The proposed frame is tested with real time datasets Here, the features of mouse action events were extracted	It takes more time to run the process. Also, only features of actions are extracted, verification frame is not implemented
Shen et al. (2016)	Permutation of conventional mouse	The trust model is built for all users, Attained high secure range. There is no specific gadget to capture or record the mouse action data	But this model is lacked standard validation and common dataset. However, it is not applicable for real time environment

[a]Few procedures of mouse dynamics

dynamics to authenticate a user via file-related operations. Features extracted are velocity, acceleration, and each mouse action curvature. A comparative study of mouse authentication based on features includes mouse action, direction, speed, acceleration, and distance that are detailed by Mondal and Bours (2013). Therefore, the planned model is used to investigate the Average Numeral of Impostor Activities (ANIA) and Average Numeral of Genuine Authenticated-users (ANGA). In this work average ANIA value is 96. Hence, the attained outcome indicates that mouse dynamics with the traditional machine learning approaches are not sufficient for continuous authentication. Moreover, the possibility of user behaviours may change from session to session also poses a problem. This also points to a hybrid system for the best option to solve this problem for non-intrusive continuous authentication.

The mouse gesture analysis for static authentication at login time is an effective approach in the biometric system. To extend this work Sayed et al. (2013) has collected data from 39 users and processed the mouse gesture method. For the gesture analysis scheme, the gesture needs to draw gestures for 8 times. Here, 14 data points samples were trained to the system then at test time the deviation from data points are calculated to authenticate the user. Finally, the mouse gesture approach has gained 0.0526% FAR and 0.0459 FRR. This method needs to be modified to make it suitable for non-intrusive continuous authentication.

Ernsberger et al. (2017) proposed mouse dynamics based on user identification from the angle of digital forensics. It has studied those user behavioural variances from interactions on different news websites. The study is different from two fundamental aspects. Firstly, the forensic evidence of a digital crime on news websites is collected and allows for timely intervention in the case of breach in security. Consequently, experiments are conducted with a small dataset that showed FAR of 0.361 and true acceptance measure as 0.439. Another work on behaviour variability is done by Cai et al. (2014), who proposed an approach using dimensionality reduction algorithms to improve authentication based on mouse dynamics. Dimensionality reduction with algorithms like multi-length scaling and Eigen maps are processed with machine learning algorithms to attain an average FAR as 0.896% and FRR as 0.774%. Finally, the planned model proved that the EER decreases with an increasing detection time. The verification system based on mouse movement curves are proposed by Hinbarji et al. (2015). It collects the data from 10 user's mouse movements and is disintegrated into a collection of curves. The outcome of this model increases the length of movement, also gained EER 0.053–0.098. In recent decades, many researchers have been utilized mouse action for user identification. Thus Shen et al. (2016) used a permutation of conventional mouse authentication using both schematic information based on mouse

Table 3 Events of mouse action captured

Feature description	Definition
Mouse event	e
Horizontal coordinate (x-axis)	x
Vertical coordinate (y-axis)	y
Timestamp	t
Starting timestamp of a sequence of movements	t_{start}
Ending timestamp of a sequence of mouse movements	t_{end}
No of mouse movements for a given event	n
No of pixels in a mouse path from origin	l
Slope angle of tangent	$\theta_i = \arctan\left(\frac{y_i}{x_i}\right)$
Average of mouse movements for each event in a given direction	$m = \frac{\sum_{i=1}^{n} x_i}{n}$
Standard deviation of mouse movement for each event	$s = \sqrt{\frac{\sum (x_i - m)^2}{n}}$
Movement offset	$O_{ij} = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2}$
Movement elapsed time (MET)	$e = t_{end} - t_{start}$
Curvature from point i to point j	$c = \frac{\theta_j - \theta_i}{l_j - l_i}$
Speed of curvature	$v = \frac{o_c}{e_c}$
Acceleration of curvature	$a = \frac{v_c}{e_c}$

trajectory and procedural information to build a trust model for every user. Subsequently, it has attained the FAR rate as 0.011 and FRR as 0.0196 with an authentication time of 6.1 s. Since the experiments were conducted in a static environment it needs to be tested on a dynamic environment to study its suitability for continuous authentication.

Mouse dynamics frame is applicable in many applications, where the action of keyboard is restricted. But the downside of the mouse-based authentication frame has a very limited number of actions to identify the own users. In spite of this drawback, the mouse authentication system is a very effective topic in continuous authentication systems (Hu et al. 2019) because of its simplicity. From this surveyed literature, it is clear that the performance indicators reported are not enough to determine which methods are the best suited for authentication purposes. Results indicate that the RF method is best suited for continuous authentication probably due to the fact that mouse sequences are a combination of limited repeated mouse actions like click and move.

3 Non-Intrusive active user authentication

In this section, the simple user authentication architecture is experimentally discussed after doing a performance analysis of the reviewed literature. The validation of the comparison result is processed with some important key metrics of the authentication process. Some of the main metrics in the user authentication system are FAR, FRR and EER. By comparing these metrics with all literature the best strategies were finalized. Hence, the non-intrusive active user authentication architecture is defined in Fig. 3.

The user login is modified to use mouse data to grant access to the resources of the system as explained by Bours and Fullu (2009). The user needs to follow the maze task, the path of user is considered as a password. The velocity of different mouse actions is calculated to build the user's signature. The experiments from this particular work could benefit by increasing the size of the dataset and the method should be modified to translate it to a real-time environment for non-intrusive continuous authentication. Henceforth, the attained EER measure is 0.2–0.4%. In another work, Ghosh et al. (2020) have been presented the authentication framework to find the own user by their handwriting styles. Moreover, the changes in character shapes might cause overlap during feature extraction. Also to estimate the performance of the proposed scheme, several user handwritings were trained and tested. Finally, it has attained the best accuracy measure for authentication. But it takes more time to execute. In addition, the key drawback behind in this authentication frame is security issues, so Ndichu et al. (2020) have been projected a fast test scheme to recognize the malicious event in the authentication framework. Henceforth, the malicious codes are detected and its process was stopped by a fast test security model. At last, it has gained high confidential measure. However, this model is complex to design.

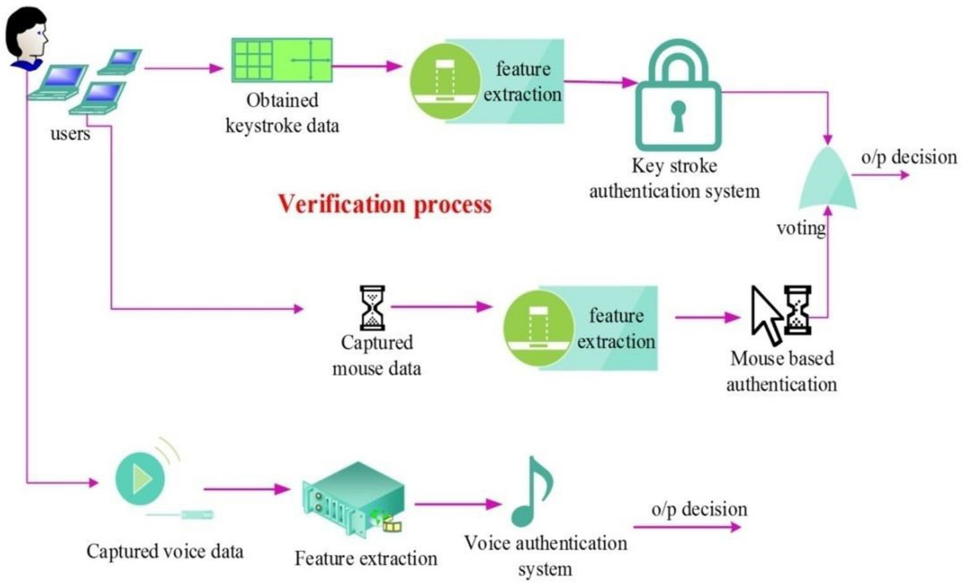


Fig. 3 Non-intrusive user authentication system architecture

Nowadays, user authentication in smartphones became a trending topic in digital field. For that, Sun et al. (2019) have been designed an authentication frame in smartphones to protect the user secrets from un-trusted parties. Here, the sensed data of own users from different mobile gadgets were trained to the system then the features of sensed data of own users were extracted using recurrent model. Hereafter, if the third party uses the smartphone then that user's actions were authenticated by matching the trained action features. In recent, to authenticate the own user Choi et al. (2019) have been introduced the signaling strategy with the support of wearable sensors. Moreover, the designed gadgets were authenticated by the users at all times. Hence, the regression analysis is utilized to extract the recorded user actions. Moreover, the signal of user's action was stored in mobile, laptop, etc. Hereafter, if any unauthenticated has tried to utilize the gadget then the specific system was locked. However, it is a long time process.

The keystroke information captured consists of event id, event name, and key location on the keyboard, ASCII code, and corresponding IBM AT code of the key pressed or released. The keystroke events are key press and release. The time of event is captured in milliseconds. The features extracted from this keystroke are press-press or P-P (time in milliseconds of first press to next press), press-release, or P-R (time in milliseconds of first press to next release), release-release, or R-R (time in milliseconds from one release to another). These feature values were calculated for monographs, digraphs, and tri-graphs. Moreover, the experimental work is done for only P-R process. The results of this study have shown in Table 3 and graphically represented in Fig. 4. The implementation simulation was done using the weka toolkit. On implementation with 5 user data, it was seen that the decision tree model, support vector scheme, and random forest algorithms gave comparable results. In that, keystroke dynamics with random forests algorithm has obtained the highest accuracy as 99.8% with monographs and tri-graphs for the press-release information. Mouse gestures were categorized into two classes namely movement without click and movement with clicks but the features were combined when implementing the authentication algorithm. Furthermore, the gained results have shown an accuracy of 97.8% using random forest method. But on increasing the size of the data it is observed that the results using the same algorithms tend to decrease up to 90.7% accuracy for keystroke dynamics tri-graph information and 91.7% for mouse dynamics for 30 users.

In keystroke dynamics, although the decision tree, random forest, and k nearest neighbour algorithms show comparable results, the neural network implementation gave a low performance. Results clearly indicate that accuracy increases in most cases while the number of features used for authentication is increased, which is shown in Table 4 and graphically represented in Figs. 4 and 5.

The results point towards the slope features of the mouse movement for better user authentication. Moreover, the mouse authentication of a different number of users is detailed in Fig. 5.

The keystroke features were calculated for monographs, digraphs, and tri-graphs. Also, authentication was implemented using decision trees, random forest, k nearest neighbour, and neural networks. Although, decision tree, random

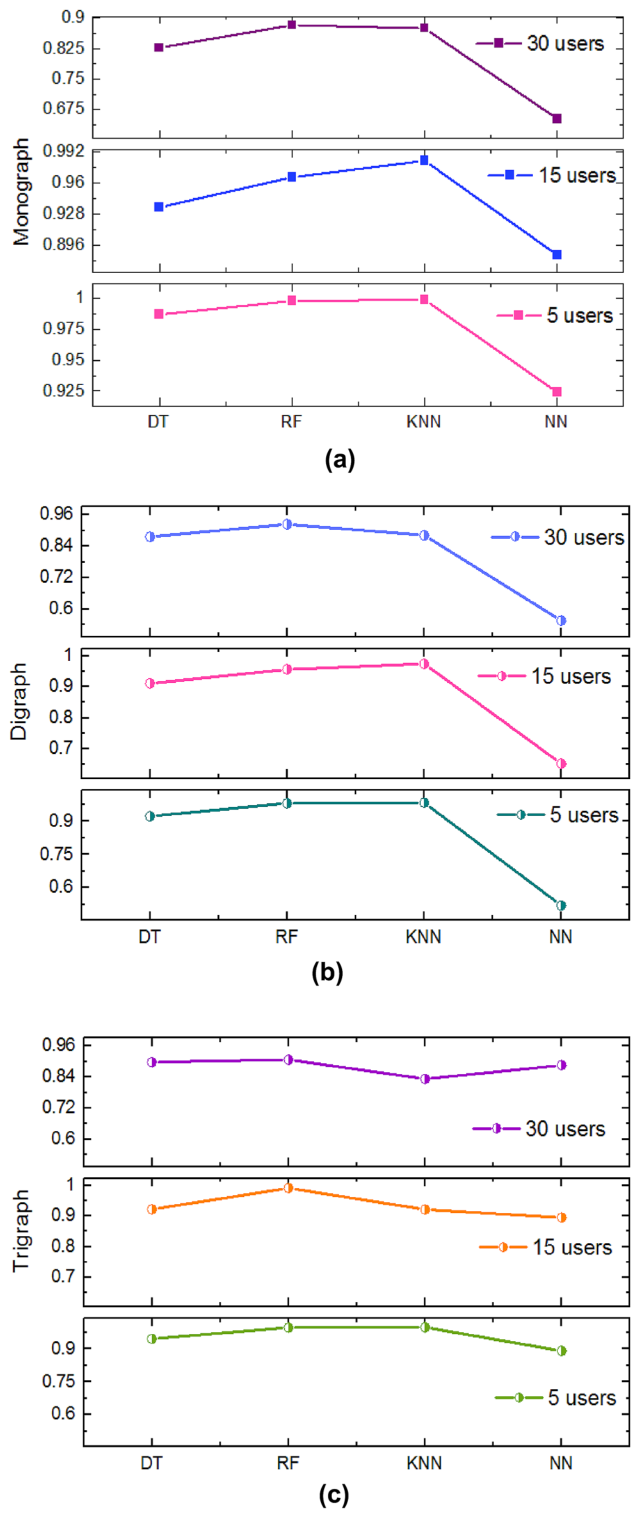


Fig. 4 Graphical representation of Keystroke authentication. **a** Monograph, **b** digraph and **c** tri-graph

forest, and k nearest neighbour algorithms have been shown the comparable results in that neural network implementation gave low performance even for the small size of the dataset. From the results validation, it is proved that the neural network implementation gave a low performance.

The authentication system has used local Fisher discriminated analysis and ISOMAP as dimensionality reduction algorithms along with classification algorithms namely KNN, Decision trees, and SVM. The investigation reports that a FAR and FRR of 0.0, when ISOMAP is used with SVM. It might be beneficial to study the method in an uncontrolled environment to identify factors that adversely affect the continuous authentication of a user. Furthermore, the verification system is vulnerable to several kinds of attacks like voice recording, keystroke and mouse action hacking, etc. Thus the common security issues in authentication systems are detailed in Fig. 6.

From the analysis, it is verified that the authentication process depends upon the trained features. If the number of users is increased then the system performance is decreased. Hence, in future incorporating maximum features in training set will improve the authentication results.

4 Overall performance assessment

To evaluate the efficiency of the keystroke dynamic system (Morales et al. 2016) analyses the results of the first Keystroke Biometrics On-going Competition (KBOC). Thus, the developed model has gained less EER as 6%. By analysis one system has got a better performance based on free environment simulation for diverse users with different passwords. The reviewed literature has proved that the keystroke analysis have the highest rank in user preference for alternative authentication with 25.5% of users (Furnell et al. 2000; Alsultan et al. 2018). The monograph in keystroke dynamics is defined as key hold time and the digraph is utilized to record the key pressed time. Moreover, the tri-graphs are designed to estimate the common features of keystrokes. Hence, in key-based authentication system, the digraphs and monographs are key parametric functions to estimate the keyboard features of each user. Furthermore, the performance of Monograph, digraph, and trigraph function using different techniques such as decision frame, RF, kernel model, and neural frame is detailed in Fig. 7. Moreover, the performance assessment of different methods using key metrics is elaborated in Table 5.

From the preliminary results, it is obvious that keystroke and mouse dynamics are good candidates for active authentication systems using a random forest algorithm. The challenge in scaling the system is to handle large amounts of data, choosing appropriate features for each biometric used, and building a system that can accommodate the user behaviour. As the continuous work, the parameter of each system should be optimized to gain the finest result. Moreover, the

Table 4 Experimental results of mouse and keystroke dynamics of the same dataset

Experimental results of mouse and keystroke dynamics of the same dataset in uncontrolled environment with different sets of user data

	Keystroke authentication									Mouse authentication			
	Monograph			Digraph			Trigraph						
Users[a]	5	15	30	5	15	30	5	15	30		5	15	30
DT	0.987	0.935	0.827	0.923	0.911	0.876	0.946	0.922	0.898	DT	0.956	0.944	0.829
RF	0.998	0.966	0.883	0.981	0.956	0.904	0.998	0.991	0.907	RF	0.978	0.934	0.917
KNN	0.999	0.983	0.875	0.984	0.974	0.882	0.999	0.921	0.833	SVM	0.958	0.956	0.899
NN	0.924	0.886	0.652	0.52	0.652	0.556	0.891	0.895	0.886	–	–	–	–

[a] Clients

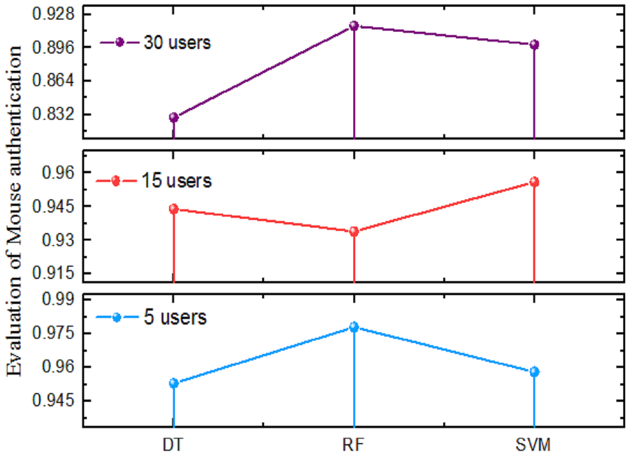


Fig. 5 Graphical representation of mouse dynamics based authentication

statistics of several authentication models are detailed in Table 6.

As mentioned earlier, the statistical approaches are not enough to represent changes in user behaviour over time because of changes in the user emotional status. An operator-dependent feature extraction technique with an existing detection algorithm (Kim et al. 2018) is also attaining a better outcome. It has reported a least mean EER of 2.95% on a keystroke length of 1000 with KNN adaptive algorithm. For a non-intrusive continuous authentication system to work effectively, the verification system should be able to implement it in real-time and any intruder must be tracked and stopped before any real damage can be done. To the best of our knowledge, none of the work so far addresses all of these requirements adequately.

The model, which has attained less error rate, can achieve better authentication performance. Moreover, that diverse model has achieved very encouraging results, acquired via a tightly controlled environment. Moreover, it has translated to a real-time uncontrolled environment to check whether it has attained similar result in real time environment. Hence, the few analysis of key and mouse dynamics system is described in Fig. 8.

For the classification model, the chief metrics are exactness measure, F-value, recall, AUC, and precision. In addition, those metrics are calculated to verify the successive rate of each authentication model that is shown in Fig. 9. Furthermore, the error in dataset training made the classification process difficult; hence the validated training and testing scores of different models are elaborated in Fig. 10.

EER is the metric that is traditionally used and calculated from FAR and FRR measures. Here first FAR and FRR were calculated for different threshold values. Hence, the FAR and FRR of different techniques are elaborated in Fig. 12. The FAR measure is calculated using Eq. (1), which is elaborated as false acceptances divided by imposter matches.

$$FAR = \frac{False\ Accep\tan ces}{Total\ imposter\ matches} \tag{1}$$

The false rejection rate is calculated using Eq. (2), which is elaborated as false rejection divided by a total number of authenticated matches.

$$FRR = \frac{False\ rejection}{Total\ authenticated\ matches} \tag{2}$$

The relationship between observed values of FAR, FRR, and EER of different datasets are detailed in Fig. 11. Authentication in biometrics is used to secure the password and other confidential data. In today's life, the biometric system plays a vital role in several applications like attendance system, e-learning, online learning assessment, remote authentication, and authorization, etc. Thus user authentication without any interruption has become more important. One of the advantages of keystroke and mouse dynamics is the process of non-intrusive does not require any special hardware. Since voice authentication is only used to break a tie in the decision, it is a good method to support the decision system.

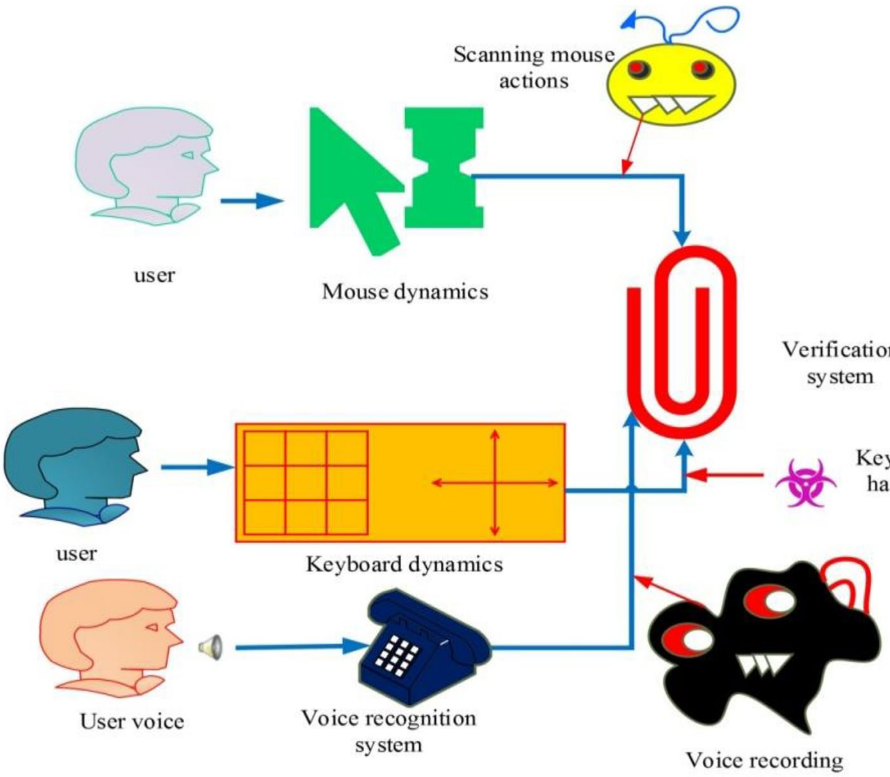


Fig. 6 Issues in verification system

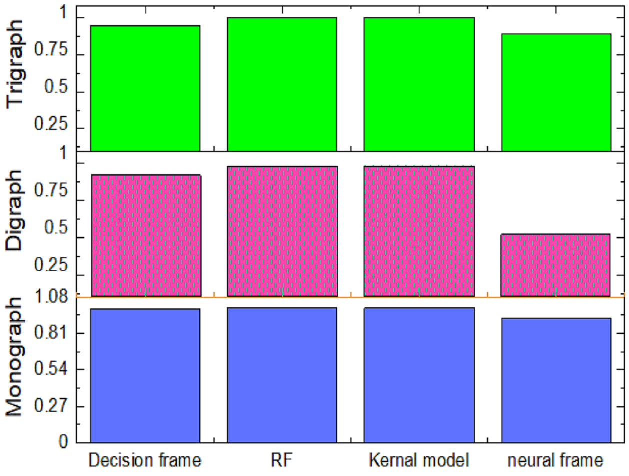


Fig. 7 Keystroke authentication process

One of the limitations of authentication system is that the behavioural dynamics of multiple users may be the same in some cases. The users may have similar motions while handling the keyboard or mouse. In that case, identifying the own user is a difficult task. So that an effective optimized ML model should be designed to tackle this drawback and to improve the system performance.

4.1 Discussion

By this review article, the advantage and disadvantages of each authentication system was analysed. Moreover, to develop the new method based on this review, the common demerits of each authentication model is detailed.

Voice biometrics The common demerit behind in this voice authentication framework is the most of systems were not automated to predict the genuine users. So, each testing the system wants to train the own user behaviour. Thus, it takes more time and needs more resources to execute the authentication process. In addition, the second drawback in this authentication system was not worked for different languages and diverse pronunciations. Moreover, if the training and testing environments are different based on the device, then the utilized algorithm has revealed very less accuracy.

Keystroke dynamics Authenticating the genuine user through the keystroke authentication frame is challengeable task in biometrics fields. Because, the typing style of the user is not same at all times it may differ based on their mental activities. Also, it lacks in security. Here, the proficient score of the developed algorithm is determined by the trained features.

Table 5 Performance and methods assessment

Authors	Data captured	Method	Analysis	Performance[a] (%)		
				FAR	FRR	EER
Gunetti and Picardi (2005)	Restricted free text Custom interface, text of 700 to 900 words	Statistics	Timing information	0.01	5	0.5
Galka et al. (2014)	Restricted free text. A collection of passwords chosen by user with length less than 20 characters are typed by user	Statistics	Timing information	0.47	0	0.1
Chang et al. (2013)	Fixed text Password	Machine learning	Timing information of tying and cognitive factors	0.055	0.03	0.6
Pisani et al. (2015)	Fixed text	Machine learning	Timing information	0.035	0.148	0.2
Agarwal and Jalal (2021)	Restricted free text	Statistical and pattern recognition	Timing information	0.025	0.026	20
Kang and Cho (2015)	Fixed text	Statistical and machine learning	Timing information	0.06	0.058	6
Morales et al. (2016)	Restricted free text	Statistical	Timing information	5.3	90.5	0.9
Li et al. (2019)	Restricted free text	Machine learning	Timing information and other non-conventional information	0.000	0.000	0.1
Tirkey and Saini (2020)	Restricted free text	Machine learning	Timing information	0.25	0.02	2.95
Lin et al. (2020)	Primary data (22 users)	Limited data, average speed per distance	ANN	2.4	6.49	2.4614
Revett et al. (2008)	6 user primary data	Information is demonstrated as digraph	statistics	0.02	0.05	2.5
Baró et al. (2020)	10 users primary data	Statistics collection mouse movement	ANN	0.055	0.03	0.3
Bours and Fullu (2009)	28 users primary data	Acceleration mouse movement	Data estimation	0.04	0.02	0.4
Jorgensen and Yu (2011)	17 users primary data	Limited data	Logic classifiers	0.03	0.03	0.49
Zheng et al. (2014)	Primary data	Angle-based metrics: way, angle of curving and bend detachment	SVM	0.05	0.04	0.013
Feher et al. (2012)	25 users	Mouse movement identification	Random forest classifier	0.08	0.09	0.1
Lin and Kumar (2018)	Primary data 20 users	mouse acceleration	Dimensionality reduction	0.0	0.0	0.12
Mondal and Bours (2013)	Primary data 49 users	Mouse action	Classifier	0.08	9.6	0.8

[a]Metrics analysis

Mouse dynamics The key drawback behind in mouse base authentication system is the mouse actions are differed from time to time. So authenticating the user based on their mouse actions or movement is difficult, also in some cases, there is possible to predict the wrong user as genuine user. Hence, the common defeats of the reviewed authentication model are detailed in Table 7.

So in future, all drawbacks of mouse-based authentication systems will be addressed by developing an optimized deep learning framework in the authentication system. Also in future, designing hybrid optimized deep learning framework based broad voice biometrics system with maximum possible pronunciation may end the issues in voice biometrics system. Furthermore, designing an optimized deep learning paradigm with security mechanism will improve the system performance of keystroke dynamics.

The trend of non-user continuous authentication based certain period is detailed in Fig. 12. Thus year to year, research works in this field are increasing in a wide range. It shows the need for user authentication in digital applications.

Table 6 Statistics of some authentication models

References[a]	Model	Score (training set)	Score (validation set)	Examine score	Measure of cross validation	Parameters	Accuracy	Precision	Recall	AUC	F-measure	Malicious scan code (%)
Shen et al. (2016)	Kernel model	0.97	0.962	0.962	0.962	Neighbours 1	95	92	70	91	79	80
Wu et al. (2016)	Logic based regression	0.96	0.961	0.953	0.967	Count 10,000	95	97	64	94	77	82
Lai et al. (2014)	Linear model	0.90	0.88	0.9	0.89	–	90	97	20	94	34	84
Rezaei et al. (2013)	Multi-layer model	0.961	0.951	0.95	0.964	Count 1000	94	97	59	94	74	84
Kambourakis et al. (2016)	Random forest model	1	0.96	0.95	0.968	Estimators 14	95	83	73	94	78	86
Giot et al. (2009)	Support vector frame	0.96	0.95	0.951	0.962	100	95	97	61	94	75	88
Kiyani et al. (2020)	Gradient boost model	0.98	0.95	0.96	0.966	Learning rate (1,0)	90	69	69	94	78	87
Sheng et al. (2005)	Decision based approach	1	0.96	0.95	0.978	Depth 3	96	97	61	94	75	86
Barkadehi et al. (2018)	Text based frame (password cracking)	0.76	0.74	0.75	–	Cracking time 60%	99	98	42	95	60	20
Rybnik et al. (2009)	Fixed text	0.76	0.75	0.1	0.75	K = 1	90	89	65	88	68	23
Shen et al. (2012)	One class analysis model	0.65	–	0.67	0.694	Training model 6	76	75	53			62
Bailey et al. (2014)	Behavioural based systems	0.74	0.73	0.65	0.72	Training statistics 30 samples	99.39	77	98	80	–	
Stanić (2013)	Application frame model	0.81	0.82	0.83	0.867	100 samples	95	97	61	94	75	88

[a]Works done in past

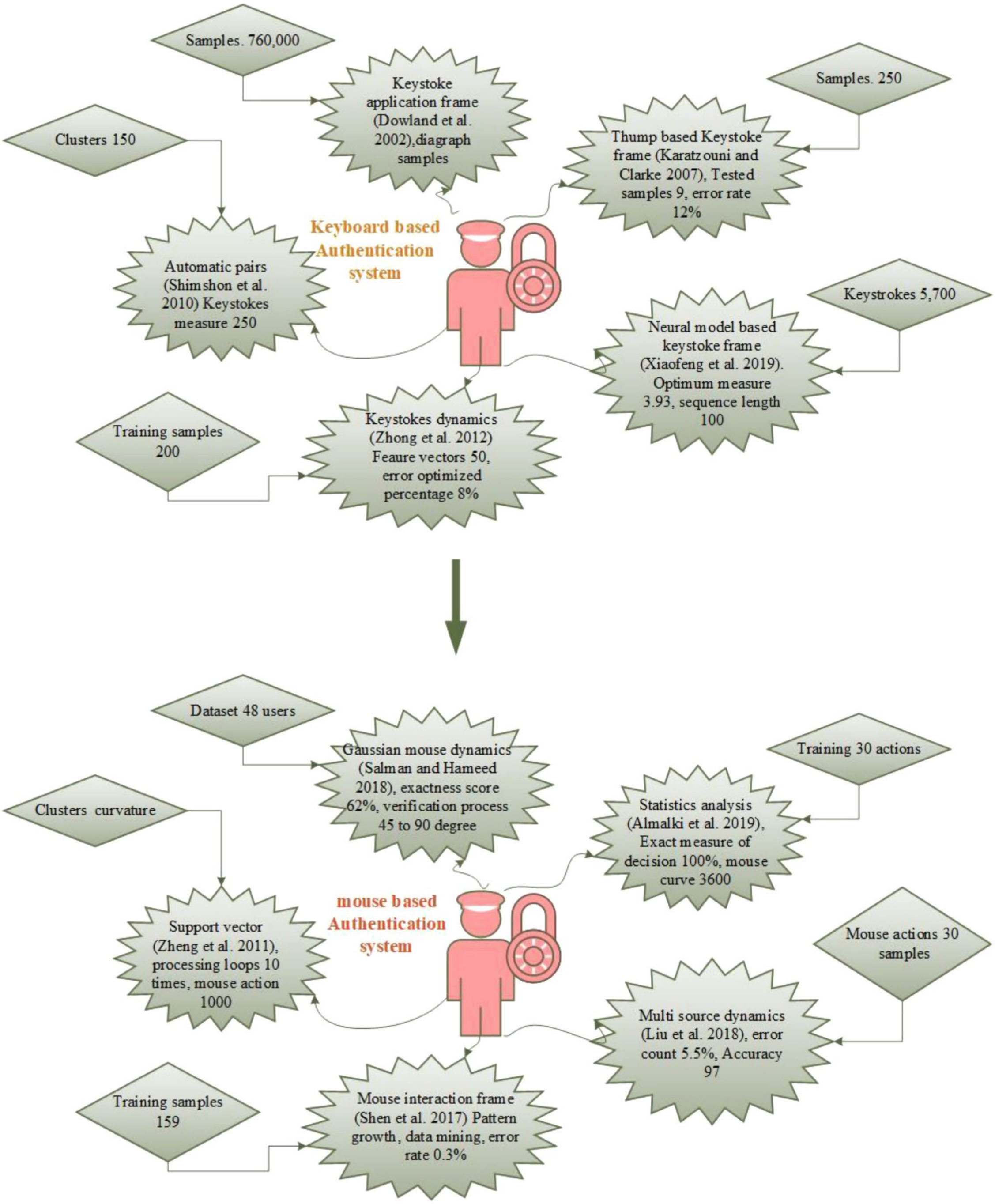

Samples. 760,000
Keystoke application frame (Dowland et al. 2002),diagraph samples
Samples. 250
Clusters 150
Thump based Keystoke frame (Karatzouni and Clarke 2007), Tested samples 9, error rate 12%
Keyboard based Authentication system
Automatic pairs (Shimshon et al. 2010) Keystokes measure 250
Keystrokes 5,700
Neural model based keystoke frame (Xiaofeng et al. 2019). Optimum measure 3.93, sequence length 100
Training samples 200
Keystokes dynamics (Zhong et al. 2012) Feaure vectors 50, error optimized percentage 8%
Dataset 48 users
Gaussian mouse dynamics (Salman and Hameed 2018), exactness score 62%, verification process 45 to 90 degree
Training 30 actions
Clusters curvature
Statistics analysis (Almalki et al. 2019), Exact measure of decision 100%, mouse curve 3600
mouse based Authentication system
Support vector (Zheng et al. 2011), processing loops 10 times, mouse action 1000
Mouse actions 30 samples
Multi source dynamics (Liu et al. 2018), error count 5.5%, Accuracy 97
Training samples 159
Mouse interaction frame (Shen et al. 2017) Pattern growth, data mining, error rate 0.3%

Fig. 8 Analysis of key and mouse dynamics authentication system

5 Conclusion

This paper has presented a comprehensive review in the area of user authentication using voice verification, keystroke, and mouse dynamics. Several models are reviewed under the user authentication section; in that, RF strategy has attained the finest outcome for all metrics. Moreover, several limitations are discussed on the impact of different types of attacks on these biometric systems and how it could be countered. These biometric methods are utilized to enable continuous or active authentication for a system to verify and identify the authenticated users. Ideally, the

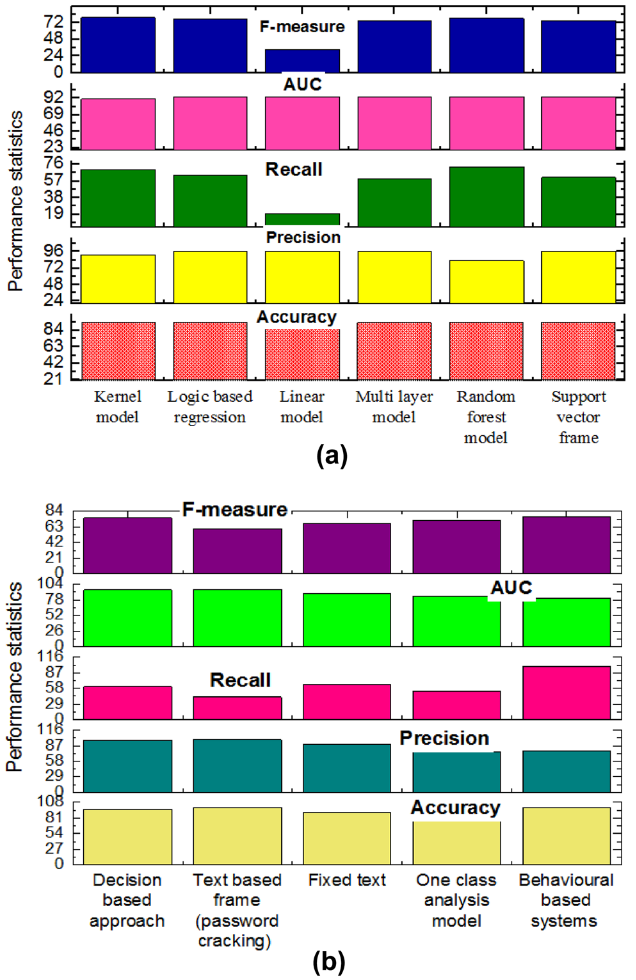


Fig. 9 Key metrics validation: **a** kernel model, logic regression, linear model, multi-layer approach, RF, support vector, **b** decision based approach, text based frame, fixed text, one class analysis frame, behavioral based scheme

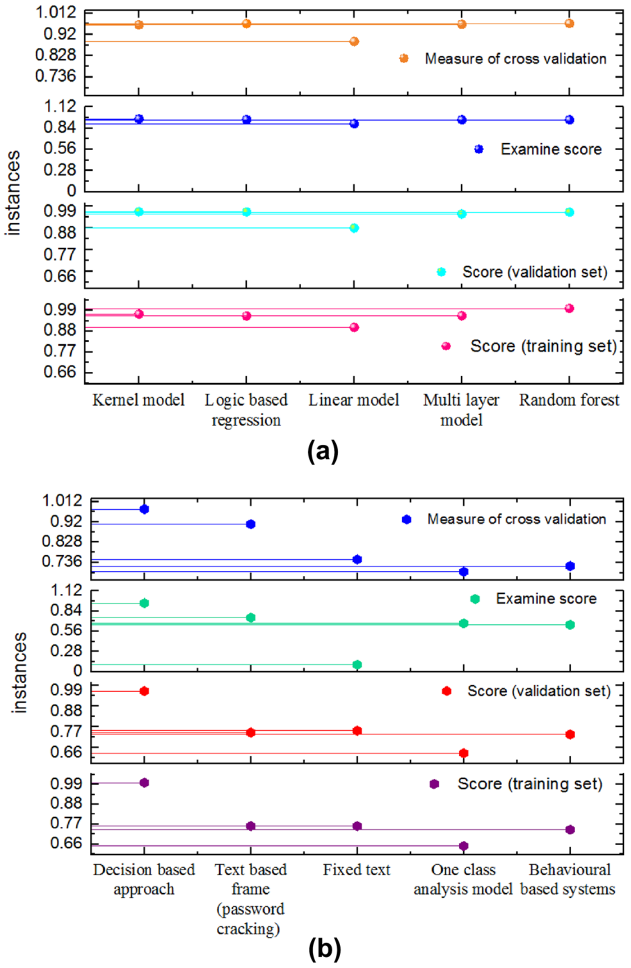


Fig. 10 Score of training and examination: **a** kernel model, logic regression, linear model, multi-layer approach, RF, support vector, **b** decision based approach, text based frame, fixed text, one class analysis frame, behavioral based scheme

system should choose the authentication method based on the active action of the user at a particular time. If the user is speaking then the system should be able to decide by speech analysis and synthesis whether the user is authentic. If the device is being used then the data captured from peripheral devices like mouse or keyboard should match to authenticate the user. In future, the design suitable deep learning model for each authentication will improve the system performance. Also tuning the key parameters of voice recognition system, mouse, and keystroke dynamics with the use of optimization framework will help to attain the best accuracy.

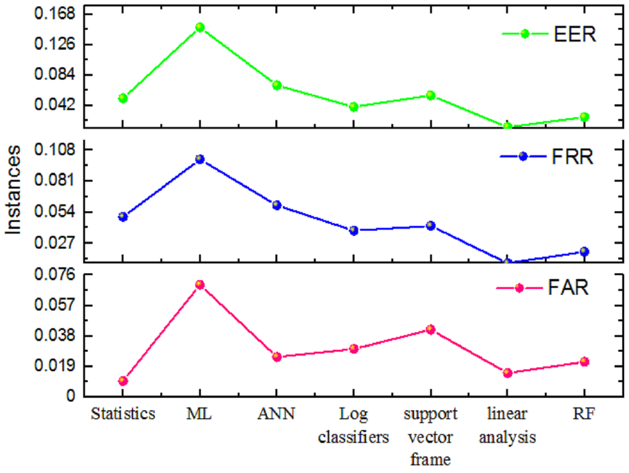


Fig. 11 Measure of EER, FRR and FAR

Table 7 Common pros and cons of behavioral biometric techniques for active authentication

Pros and cons[a] of behavioral biometric system for active authentication

Behavioral biometric	Operating method	Prominent algorithm	Pros	Cons
Voice biometric recognition	Text independent speaker verification	Gaussian mixture model	Input can be hands off through microphone Unique speech patterns can be used for secure access Can be used by people with physical handicap Suitable for remote access Many devices have built in voice recognition	System needs to be trained separately for each user System may not work for different pronunciations and languages FRR is generally high especially with external noise Algorithms show less accuracy when training and testing environment differs
Keystroke dynamics	Free text	SVM	Discriminative capacity Low cost since no extra hardware needed Adds to traditional security systems Time to identify intruder is comparatively less	Tends to change quickly over time Performance depends on several extraneous factors like mental state of the user. Security issues are not widely addressed Comparatively few research on free text The efficiency of the Algorithm depends on the used or trained features
Mouse dynamics	Dynamic mouse movement	RF	Used for most system activity Discriminative capacity Enhance security Non-intrusive	Limited range of activities Time to time the actions are differed Performance depends on factors like distance from the mouse, state of mind, and so on Security issues need to be researched Algorithm efficiency depends on features used Time to identify intruder is generally high

[a] Advantages and disadvantages

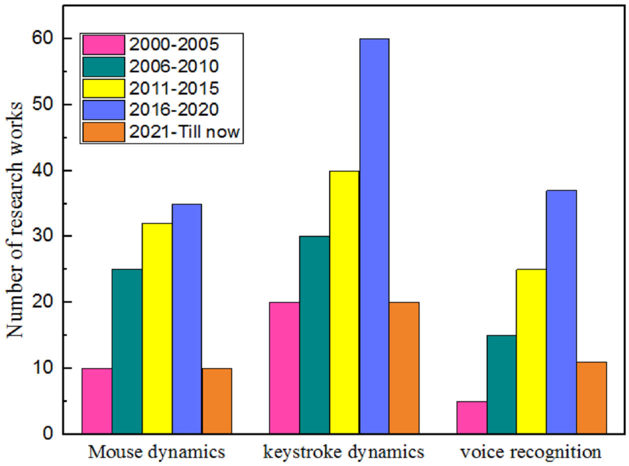


Fig. 12 Trend of research works towards non-user continuous authentication by voice recognition, mouse and keystroke dynamics

Declarations

Conflict of interest The authors declare that they have no potential conflict of interest.

Statement of human and animal rights/ethical approval All applicable institutional and/or national guidelines for the care and use of animals were followed.

Informed consent For this type of study formal consent is not required.

References

Abdul-Hassan AK, Hadi IH (2020) A proposed authentication approach based on voice and fuzzy logic. Recent trends in intelligent computing, communication and devices. Springer, Singapore, pp 489–502. https://doi.org/10.1007/978-981-13-9406-5_60

Agarwal R, Jalal AS (2021) Presentation attack detection system for fake Iris: a review. Multimed Tools Appl 80:15193–15214. https://doi.org/10.1007/s11042-020-10378-7

Ahmed AAE, Traore I (2007) A new biometric technology based on mouse dynamics. IEEE Trans Depend Secure Comput. https://doi.org/10.1109/TDSC.2007.70207

Ali ML, Monaco JV, Tappert CC, Qiu M (2017) Keystroke biometric systems for user authentication. J Signal Process Syst 86(2–3):175–190. https://doi.org/10.1007/s11265-016-1114-9

Ali ABA, Ponnusamay V, Sangodiah A (2019) User behaviour-based mobile authentication system. In: Advances in computer communication and computational sciences. Springer, Singapore, pp 461–472. https://doi.org/10.1007/978-981-13-6861-5_40

Almaadeed N, Aggoun A, Amira A (2012) Audio-visual feature fusion for speaker identification. In: International conference on neural information processing. Springer, Berlin. https://doi.org/10.1007/978-3-642-34475-6_8

Almalki S, Chatterjee P, Roy K (2019) Continuous authentication using mouse clickstream data analysis. In: International conference on security, privacy and anonymity in computation, communication and storage. Springer, Cham. https://doi.org/10.1007/978-3-030-24900-7_6

Alshehri A, Coenen F, Bollegala D (2017) Accurate continuous and non-intrusive user authentication with multivariate keystroke streaming. In: Proceedings of the 9th international joint conference on knowledge discovery, knowledge engineering and knowledge management. SCITEPRESS-Science and Technology Publications

Alsultan A, Warwick K, Wei H (2018) Improving the performance of free-text keystroke dynamics authentication by fusion. Appl Soft Comput 70:1024–1033. https://doi.org/10.1016/j.asoc.2017.11.018

Antal M, Egyed-Zsigmond E (2019) Intrusion detection using mouse dynamics. IET Biometr 8(5):285–294. https://doi.org/10.1049/iet-bmt.2018.5126

Bailey KO, Okolica JS, Peterson GL (2014) User identification and authentication using multi-modal behavioral biometrics. Comput Secur 43:77–89. https://doi.org/10.1016/j.cose.2014.03.005

Barkadehi MH, Nilashi M, Ibrahim O, Fardi AZ (2018) Authentication systems: a literature review and classification. Telemat Inform 35(5):1491–1511. https://doi.org/10.1016/j.tele.2018.03.018

Baró X, Bernaus RM, Baneres D (2020) Biometric tools for learner identity in e-assessment. In: Engineering data-driven adaptive trust-based e-assessment systems. Springer, Cham, pp 41–65. https://doi.org/10.1007/978-3-030-29326-0_3

Belman AK, Sridhara S, Phoha VV (2020) Classification of threat level in typing activity through keystroke dynamics. In: 2020 International conference on artificial intelligence and signal processing (AISP), IEEE. https://doi.org/10.1109/AISP48273.2020.9073079

Bernabe JB, David M, Moreno RT, Cordero JP (2020) Aries: evaluation of a reliable and privacy-preserving European identity management framework. Future Gener Comput Syst 102:409–425. https://doi.org/10.1016/j.future.2019.08.017

Bidgoly AJ, Bidgoly HJ, Arezoumand Z (2020) A survey on methods and challenges in EEG based authentication. Comput Secur. https://doi.org/10.1016/j.cose.2020.101788

Bours P, Fullu CJ (2009) A login system using mouse dynamics. In: 2009 Fifth international conference on intelligent information hiding and multimedia signal processing, Kyoto, pp 1072–1077. https://doi.org/10.1109/IIH-MSP.2009.77

Cai Z, Shen C, Guan X (2014) Mitigating behavioral variability for mouse dynamics: a dimensionality-reduction-based approach. IEEE Trans Hum Mach Syst 44(2):244–255. https://doi.org/10.1109/THMS.2014.2302371

Cao Y, Zhang Q, Li F, Yang S (2020) PPGPass: nonintrusive and secure mobile two-factor authentication via wearables. In: IEEE INFOCOM 2020-IEEE conference on computer communications, IEEE. https://doi.org/10.1109/INFOCOM41043.2020.9155380

Chang JM, Fang CC, Ho KH, Kelly N et al (2013) Capturing cognitive fingerprints from keystroke dynamics. IEEE Comput Soc 15:24

Choi GH, Jung JH et al (2019) User authentication system based on baseline-corrected ECG for biometrics. Intell Autom Soft Comput 25(1):193–204

Chong P, Elovici Y, Binder A (2019) User authentication based on mouse dynamics using deep neural networks: a comprehensive study. IEEE Trans Inf Forensics Secur 15:1086–1101. https://doi.org/10.1109/TIFS.2019.2930429

Clarke NL, Furnell SM (2007) Advanced user authentication for mobile devices. Comput Secur 26(2):109–119. https://doi.org/10.1016/j.cose.2006.08.008

Clarke NL, Furnell SM, Rodwell PM, Reynolds PL (2002) Acceptance of subscriber authentication methods for mobile telephony devices. Comput Secur 21(3):220–228. https://doi.org/10.1016/S0167-4048(02)00304-8

Clarke N, Karatzouni S, Furnell S (2009) Flexible and transparent user authentication for mobile devices. In: IFIP international information security conference. Springer, Berlin. https://doi.org/10.1007/978-3-642-01244-0_1

Dobbie S (2020) Challenge of biometric security for banks. Biometric Technol Today 2020(3):5–7. https://doi.org/10.1016/S0969-4765(20)30037-0

Dowland PS, Furnell SM, Papadaki M (2002) Keystroke analysis as a method of advanced user authentication and response. In: Security in the information society. Springer, Boston, pp 215–226. https://doi.org/10.1007/978-0-387-35586-3_17

Ernsberger D, Ikuesan RA, Venter SH (2017) A web-based mouse dynamics visualization tool for user attribution in digital forensic readiness. In: International conference on digital forensics and cyber crime. Springer, Cham. https://doi.org/10.1007/978-3-319-73697-6_5

Feher C, Elovici Y, Moskovitch R, Rokach L, Schclar A (2012) User identity verification via mouse dynamics. Inf Sci 201:19–36. https://doi.org/10.1016/j.ins.2012.02.066

Ferrag MA, Maglaras L, Derhab A, Janicke H (2020) Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues. Telecommun Syst 73(2):317–348. https://doi.org/10.1007/s11235-019-00612-5

Fourati E, Elloumi W, Chetouani A (2020) Anti-spoofing in face recognition-based biometric authentication using Image Quality Assessment. Multimed Tools Appl 79(1–2):865–889. https://doi.org/10.1007/s11042-019-08115-w

Furnell SM, Dowland PS, Illingworth HM, Reynolds PL (2000) Authentication and supervision: a survey of user attitudes. Comput Secur 19(6):529–539. https://doi.org/10.1016/S0167-4048(00)06027-2

Furnell S, Clarke N, Karatzouni S (2008) Beyond the pin: enhancing user authentication for mobile devices. Comput Fraud Secur 2008(8):12–17. https://doi.org/10.1016/S1361-3723(08)70127-1

Galka J, Masior M, Salasa M (2014) Voice authentication embedded solution for secured access control. IEEE Trans Consum Electron 60(4):653–651. https://doi.org/10.1109/TCE.2014.7027339

Gao L, Lian Y, Yang H, Xin R, Yu Z (2020) Continuous authentication of mouse dynamics based on decision level fusion. In: 2020 International wireless communications and mobile computing (IWCMC), IEEE. https://doi.org/10.1109/IWCMC48107.2020.9148499

Ghosh S, Shivakumara P et al (2020) Graphology based handwritten character analysis for human behaviour identification. CAAI Trans Intell Technol 5(1):55–65

Giot R, El-Abed M, Rosenberger C (2009) Keystroke dynamics with low constraints svm based passphrase enrolment. In: 2009 IEEE 3rd international conference on biometrics: theory, applications, and systems, IEEE. https://doi.org/10.1109/BTAS.2009.5339028

Gunetti D, Picardi C (2005) Keystroke analysis of free text. ACM Trans Inf Syst Secur 8(3):312–347. https://doi.org/10.1145/1085126.1085129

Gupta S, Buriro A, Crispo B (2020) A chimerical dataset combining physiological and behavioral biometric traits for reliable user authentication on smart devices and ecosystems. Data Brief 28:104924. https://doi.org/10.1016/j.dib.2019.104924

Hinbarji Z, Albatal R, Gurrin C (2015) Dynamic user authentication based on mouse movements curves. In: International conference on multimedia modeling. Springer, Cham. https://doi.org/10.1007/978-3-319-14442-9_10

Hu T, Niu W, Zhang X, Liu X, Lu J, Liu Y (2019) An insider threat detection approach based on mouse dynamics and deep learning. Secur Commun Netw. https://doi.org/10.1155/2019/3898951

Jagadeesan H, Hsiao MS (2009) A novel approach to design of user re-authentication systems. In: 2009 IEEE 3rd international conference on biometrics: theory, applications, and systems, IEEE. https://doi.org/10.1109/BTAS.2009.5339075

Jorgensen Z, Yu T (2011) On mouse dynamics as a behavioral biometric for authentication. In: Proceedings of the 6th ACM symposium on information, computer and communications security (ASIACCS '11), ACM, New York, NY, USA, pp 476–482. https://doi.org/10.1145/1966913.1966983

Kambourakis G, Damopoulos D, Papamartzivanos D, Pavlidakis E (2016) Introducing touchstroke: keystroke-based authentication system for smartphones. Secur Commun Netw 9(6):542–554. https://doi.org/10.1002/sec.1061

Kang P, Cho S (2015) Keystroke dynamics-based user authentication using long and free text strings from various input devices. Inf Sci 308:72–93. https://doi.org/10.1016/j.ins.2014.08.070

Karatzouni S, Clarke N (2007) Keystroke analysis for thumb-based keyboards on mobile devices. In: IFIP international information security conference. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-72367-9_22

Kasprowski P, Harezlak K (2018) Fusion of eye movement and mouse dynamics for reliable behavioral biometrics. Pattern Anal Appl 21(1):91–103. https://doi.org/10.1007/s10044-016-0568-5

Kaur H, Khanna P (2020) Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing. Future Gener Comput Syst 102:30–41. https://doi.org/10.1016/j.future.2019.07.023

Kaur R, Sandhu RS, Gera A, Kaur T, Gera P (2020) Intelligent voice bots for digital banking. In: Smart systems and IoT: innovations in computing. Springer, Singapore, pp 401–408. https://doi.org/10.1007/978-981-13-8406-6_38

Kim DH, Lee J, Yoon HS, Cha EY (2007) A non-cooperative user authentication system in robot environments. IEEE Trans Consum Electron 53(2):804–811. https://doi.org/10.1109/TCE.2007.381763

Kim J, Kim H, Kang P (2018) Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection. Appl Soft Comput 62:1077–1087. https://doi.org/10.1016/j.asoc.2017.09.045

Kim JS, Choi GH, Pan SB (2019) A Study on electrocardiogram based biometrics using embedded module. In: 2019 International conference on platform technology and service (PlatCon), IEEE. https://doi.org/10.1109/PlatCon.2019.8669422

Kiyani AT, Lasebae A, Ali K, Rehman MU, Haq B (2020) Continuous user authentication featuring keystroke dynamics based on robust recurrent confidence model and ensemble learning approach. IEEE Access 8:156177–156189. https://doi.org/10.1109/ACCESS.2020.3019467

Kuppusamy KS (2019) PassContext and PassActions: transforming authentication into multi-dimensional contextual and interaction sequences. J Ambient Intell Hum Comput. https://doi.org/10.1007/s12652-019-01336-9

Lai WK, Tan BG, Soo MS, Khan I (2014) Two-factor user authentication with the CogRAM weightless neural net. In: 2014 International joint conference on neural networks (IJCNN), IEEE. https://doi.org/10.1109/IJCNN.2014.6889702

Lakshmi C, Ravi VM, Thenmozhi K, Rayappan JBB (2020) Con (dif) fused voice to convey secret: a dual-domain approach. Multimed Syst. https://doi.org/10.1007/s00530-019-00644-6

Lang D, van der Haar D (2020) Recommendations for biometric access control system deployment in a vehicle context in South Africa. In: Information science and applications. Springer, Singapore, pp 305–317. https://doi.org/10.1007/978-981-15-1465-4_32

Lee K, Yim K (2020) Cybersecurity threats based on machine learning-based offensive technique for password authentication. Appl Sci 10(4):1286. https://doi.org/10.3390/app10041286

Li X, Peng J, Obaidat MS, Wu F, Khan MK et al (2019) A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. IEEE Syst J 14(1):39–50. https://doi.org/10.1109/JSYST.2019.2899580

Lin C, Kumar A (2018) Matching contactless and contact-based conventional fingerprint images for biometrics identification. IEEE Trans Image Process 27(4):2008–2021. https://doi.org/10.1109/TIP.2017.2788866

Lin C, Chang C, Liang D (2012) A new non-intrusive authentication approach for data protection based on mouse dynamics. In: 2012 International symposium on biometrics and security technologies, Taipei, pp 9–14. https://doi.org/10.1109/ISBAST.2012.11

Lin CC, Chang CC, Liang D (2013) A novel non-intrusive user authentication method based on touchscreen of smartphones. In: 2013 International symposium on biometrics and security technologies, IEEE.https://doi.org/10.1109/ISBAST.2013.37

Lin Z, Meng W, Li W, Wong DS (2020) Developing cloud-based intelligent touch behavioral authentication on mobile phones. Deep biometrics. Springer, Cham. https://doi.org/10.1007/978-3-030-32583-1_7

Ling CH, Lee CC, Yang CC, Hwang MS (2017) A secure and efficient one-time password authentication scheme for WSN. IJ Netw Secur 19(2):177–181

Lipke-Perry T, Dutto DJ, Levy M (2019) The piano keyboard as task constraint: timing patterns of pianists' scales persist across instruments. Music Sci 2:2059204319870733. https://doi.org/10.1177/2059204319870733

Liu X, Shen C, Chen Y (2018) Multi-source interactive behavior analysis for continuous user authentication on smartphones. In: Chinese conference on biometric recognition. Springer, Cham. https://doi.org/10.1007/978-3-319-97909-0_71

Medikonda J, Bhardwaj S, Madasu H (2020) An information set-based robust text-independent speaker authentication. Soft Comput 24(7):5271–5287. https://doi.org/10.1007/s00500-019-04277-9

Messerman A, Mustafić T, Camtepe SA (2011) Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics. In: 2011 International joint conference on biometrics (IJCB), IEEE. https://doi.org/10.1109/IJCB.2011.6117552

Mishra V, Gupta R, Sood G, Patni JC (2018) User authentication using keystroke dynamics. Recent Trends Sci Technol Manag Soc Dev 73

Mondal S, Bours P (2013) Continuous authentication using mouse dynamics. In: 2013 International conference of the BIOSIG special interest group (BIOSIG), Darmstadt, pp 1–12

Morales A, Fierrez J, Tolosana R, Ortega-Garcia J (2016) Keystroke biometrics ongoing competition. IEEE Access 4:7736–7746. https://doi.org/10.1109/ACCESS.2016.2626718

Moreno-Rodriguez JC, Ramirez-Cortes JM (2020) Bimodal biometrics using EEG-voice fusion at score level based on hidden Markov models. In: Intuitionistic and type-2 fuzzy logic enhancements in neural and optimization algorithms: theory and applications. Springer, Cham, pp 645–657. https://doi.org/10.1007/978-3-030-35445-9_44

Navarro EC, García ML, Lara RR, Reíllo RS (2015) Flexible biometric online speaker-verification system implemented on FPGA using vector floating-point units. IEEE Trans Very Large Scale (VLSI) Integr Syst 23(11):2497–2507. https://doi.org/10.1109/TVLSI.2014.2377578

Ndichu S, Kim S, Ozawa S (2020) Deobfuscation, unpacking, and decoding of obfuscated malicious JavaScript for machine learning models detection performance improvement. CAAI Trans Intell Technol 5(3):184–192

Partila P, Tovarek J, Ilk GH, Rozhon J (2020) Deep learning serves voice cloning: how vulnerable are automatic speaker verification systems to spoofing trials? IEEE Commun Mag 58(2):100–105. https://doi.org/10.1109/MCOM.001.1900396

Patro KK, Reddi SPR, Khalelulla SKE, Rajesh Kumar P, Shankar K (2020) ECG data optimization for biometric human recognition using statistical distributed machine learning algorithm. J Supercomput 76(2):858–875. https://doi.org/10.1007/s11227-019-03022-1

Pisani PH, Lorena AC et al (2015) Ensemble of adaptive algorithms for keystroke dynamics. In: 2015 Brazilian conference on intelligent systems (BRACIS), Natal, pp 310–315. https://doi.org/10.1109/BRACIS.2015.29

Rakshit S (2020) User identification and authentication through voice samples. In: Computational intelligence in pattern recognition. Springer, Singapore, pp 247–254. https://doi.org/10.1007/978-981-13-9042-5_21

Revett K, Jahankhani H, de Magalhaes ST, Henrique S (2008) A survey of user authentication based on mouse dynamics. Glob E-Secur 12:210–219. https://doi.org/10.1007/978-3-540-69403-8_25

Rezaei A, Mirzakuchaki S (2013) A recognition approach using multilayer perceptron and keyboard dynamics patterns. In: 2013 First Iranian conference on pattern recognition and image analysis (PRIA), IEEE. https://doi.org/10.1109/PRIA.2013.6528445

Rodwell PM, Furnell SM, Reynolds PL (2007) A non-intrusive biometric authentication mechanism utilising physiological characteristics of the human head. Comput Secur 26(7–8):468–478. https://doi.org/10.1016/j.cose.2007.10.001

Roth J, Liu X, Ross A, Metaxas D (2013) Biometric authentication via keystroke sound. In: 2013 international conference on biometrics (ICB), IEEE. https://doi.org/10.1109/ICB.2013.6613015

Rude M (2019) Using the QWERTY keyboard as a chord keyboard: syllabic typing by multi-key strokes for language learning & more. In: AI and machine learning in language education, pp 168–180.

Rybnik M, Panasiuk P, Saeed K (2009) User authentication with keystroke dynamics using fixed text. In: 2009 International conference on biometrics and kansei engineering, IEEE. https://doi.org/10.1109/ICBAKE.2009.42

Saevanee H, Clarke N, Furnell S, Biscione V (2015) Continuous user authentication using multi-modal biometrics. Comput Secur 53:234–246. https://doi.org/10.1016/j.cose.2015.06.001

Salman OA, Hameed SM (2018) Using mouse dynamics for continuous user authentication. In: Proceedings of the future technologies conference. Springer, Cham. https://doi.org/10.1007/978-3-030-02686-8_58

Sayed B, Traoré I, Woungang I, Obaidat MS (2013) Biometric authentication using mouse gesture dynamics. IEEE Syst J 7(2):262–274. https://doi.org/10.1109/JSYST.2012.2221932

Shen C, Cai Z, Guan X, Sha H, Du J (2009) Feature analysis of mouse dynamics in identity authentication and monitoring. In: 2009 IEEE international conference on communications, Dresden, pp 1–5. https://doi.org/10.1109/ICC.2009.5199032

Shen C, Cai Z, Guan X, Du Y (2012) User authentication through mouse dynamics. IEEE Trans Inf Forensics Secur 8(1):16–30. https://doi.org/10.1109/TIFS.2012.2223677

Shen C, Cai Z, Liu X, Guan X, Maxion RA (2016) MouseIdentity: modeling mouse-interaction behavior for a user verification system. IEEE Trans Hum Mach Syst 46(5):734–748. https://doi.org/10.1109/THMS.2016.2558623

Shen C, Chen Y, Guan X (2017) Pattern-growth based mining mouse-interaction behavior for an active user authentication system. IEEE Trans Depend Secure Comput. https://doi.org/10.1109/TDSC.2017.2771295

Sheng Y, Phoha VV, Rovnyak SM (2005) A parallel decision tree-based method for user authentication based on keystroke patterns. IEEE Trans Syst Man Cybern Part B (cybernetics) 35(4):826–833. https://doi.org/10.1109/TSMCB.2005.846648

Shimshon T, Moskovitch R, Rokach L (2010) Continuous verification using keystroke dynamics. In: 2010 International conference on computational intelligence and security, IEEE. https://doi.org/10.1109/CIS.2010.95

Shirvanian M, Vo S, Saxena N (2019) Quantifying the breakability of voice assistants. In: 2019 IEEE international conference on pervasive computing and communications (PerCom), IEEE. https://doi.org/10.1109/PERCOM.2019.8767399

Sholokhov A, Kinnunen T, Vestman V (2020) Voice biometrics security: extrapolating false alarm rate via hierarchical Bayesian modeling of speaker verification scores. Comput Speech Lang 60:101024. https://doi.org/10.1016/j.csl.2019.101024

Sinigaglia F, Carbone R, Costa G, Zannone N (2020) A survey on multi-factor authentication for online banking in the wild. Comput Secur 95:101745. https://doi.org/10.1016/j.cose.2020.101745

Sizov A, Khoury E, Kinnunen T, Wu Z, Marcel S (2015) Joint speaker verification and anti-spoofing in the i-vector space. IEEE Trans Inf Forensics Secur 10(4):821–832. https://doi.org/10.1109/TIFS.2015.2407362

Stanić M (2013) Continuous user verification based on behavioral biometrics using mouse dynamics. In: Proceedings of the ITI 2013 35th international conference on information technology interfaces, IEEE. https://doi.org/10.2498/iti.2013.0505

Sun Y, Gao Q, Du X, Gu Z (2019) Smartphone user authentication based on holding position and touch-typing biometrics. Comput Mater Continua 3(61):1365–1375

Tan YXM, Iacovazzi A, Homoliak I (2019) Adversarial attacks on remote user authentication using behavioural mouse dynamics. In: 2019 International joint conference on neural networks (IJCNN), IEEE. https://doi.org/10.1109/IJCNN.2019.8852414

Teh PS, Zhang N, Tan SY et al (2019) Strengthen user authentication on mobile devices by using user's touch dynamics pattern. J Ambient Intell Hum Comput. https://doi.org/10.1007/s12652-019-01654-y

Tirkey BB, Saini BS (2020) Proposing model for recognizing user position. In: First international conference on sustainable technologies for computational intelligence. Advances in intelligent systems and computing, vol 1045. Springer, Singapore. https://doi.org/10.1007/978-981-15-0029-9_12

Verwey WB (2019) Isoluminant stimuli in a familiar discrete keying sequence task can be ignored. Psychol Res 85:1–15

Vestman V, Kinnunen T, Hautamäki RG (2020) Voice mimicry attacks assisted by automatic speaker verification. Comput Speech Lang 59:36–54. https://doi.org/10.1016/j.csl.2019.05.005

Vittori P (2019) Ultimate password: is voice the best biometric to beat hackers? Biometr Technol Today 2019(9):8–10. https://doi.org/10.1016/S0969-4765(19)30127-4

Wang X, Guo F, Ma JF (2012) User authentication via keystroke dynamics based on difference subspace and slope correlation degree. Digit Signal Process 22(5):707–712. https://doi.org/10.1016/j.dsp.2012.04.012

Wu PY, Fang CC, Chang JM (2016) Cost-effective kernel ridge regression implementation for keystroke-based active authentication system. IEEE Trans Cybern 47(11):3916–3927. https://doi.org/10.1109/TCYB.2016.2590472

Xiaofeng L, Shengfei Z, Shengwei Y (2019) Continuous authentication by free-text keystroke based on CNN plus RNN. Procedia Comput Sci 147:314–318. https://doi.org/10.1016/j.procs.2019.01.270

Yıldırım M, Anarım E (2019) Session-based user authentication via mouse dynamics. In: 2019 27th signal processing and communications applications conference (SIU), IEEE. https://doi.org/10.1109/SIU.2019.8806286

Zheng N, Paloski A, Wang H (2011) An efficient user verification system via mouse movements. In: Proceedings of the 18th ACM conference on Computer and communications security (CCS '11), ACM, New York, NY, USA, pp 139–150. https://doi.org/10.1145/2046707.2046725

Zheng N, Bai K, Huang H (2014) You are how you touch: user verification on smartphones via tapping behaviors. In: 2014 IEEE 22nd international conference on network protocols, IEEE. https://doi.org/10.1109/ICNP.2014.43

Zhong Y, Deng Y, Jain AK (2012) Keystroke dynamics for user authentication. In: 2012 IEEE computer society conference on computer vision and pattern recognition workshops, IEEE. https://doi.org/10.1109/CVPRW.2012.6239225

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.