IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 8 January 2023, accepted 23 February 2023, date of publication 6 March 2023, date of current version 15 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3253484

SURVEY

A Comprehensive Survey of Context-Aware Continuous Implicit Authentication in Online Learning Environments

RISEUL RYU, SOONJA YEOM, (Member, IEEE), DAVID HERBERT, AND JULIAN DERMOUDY
School of ICT, University of Tasmania, Hobart, TAS 7000, Australia

Corresponding author: Riseul Ryu (riseul.ryu@utas.edu.au)

ABSTRACT User authentication is crucial in the digital learning environment to preserve the integrity and reliability of the learning process. Implicit authentication using biometrics has been proposed to improve the user experience while resolving the issues that password dominant authentication faces. Implicit authentication does not require explicit user actions as it is a background process that implicitly acquires a user's identifying information through sensors embedded within the authenticating devices. To accommodate a variety of user contexts, context-aware implicit authentication has gained attention—especially in the mobile device domain—but it has not been fully explored in digital learning environments. This study is motivated to determine how implicit authentication can observe students' behaviour without causing disruption to their learning activity. The study provides a structured systematic review of the existing literature to identify and discuss the structure of context-aware continuous implicit authentication systems and future directions. The study found that requirements in the future will be: 1) to consider diverse authenticators to cover all possible user interactions with online learning environments, including coverage of course participants not engaged with online exams; 2) to investigate template adaptation to overcome template ageing issues with biometrics; and 3) to explore evaluation approaches of context-aware implicit authentication systems.

INDEX TERMS Biometric (access control), context-aware, implicit authentication, online learning.

I. INTRODUCTION

The transition from face-to-face learning and teaching to online learning (E-learning) or blended learning has been the subject of considerable interest over the last couple of decades [1] and it has been accelerated recently by the COVID-19 pandemic [2], [3]. In the current climate, online learning and teaching have become common practice. Moreover, numerous methodologies and learning management systems have been introduced and applied to deliver and promote online learning successfully [4], [5]. With the opportunities and benefits of online learning, there are also unique challenges encountered including, for example, content management, effective invigilation of online exams, and online lecture delivery [4]. Among different challenges in online learning environments, the critical risks unique to online learning models are, impersonation and weak authentication, which lead to poor trust in the security and integrity of the online learning model [6]. It is important to ensure that the person accessing the course resources and performing learning activities is enrolled in the course [5]. Therefore, authentication is the key aspect of online learning as a means to retain the integrity, reliability, and transparency of the learning process [6], [7].

Most online learning management systems allow learners to log in to their own course through authentication. Different authentication mechanisms can be applied in online learning environments including (1) knowledge based (what a user knows), (2) possession based (what a user has) and (3) biometrics based (what a user is) [3]. Knowledge based authentication using usernames and passwords (also known as password-based) is the most widely applied authentication

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

method, but passwords can potentially be vulnerable and stolen, leading to a failure to authenticate the genuine learner [8], [9], [10]. The prime example where this is of concern involves academic integrity — consider that learner A (who is the genuine enrolled student) provides their authentication credentials to person B (an imposter), who then completes some or all of the learning activities and assessments required instead of learner A. Such a scenario may be partially mitigated by using the unique physiological characteristics of an individual (e.g., face or fingerprint) for authentication; therefore, it cannot be shared with others and it is much more difficult to falsely claim the identity [11]. However, it is only a partial mitigation strategy as such authentication occurs only at login time paving the way for the possibility of impersonation to occur after the initial login phase [12]. For instance, learner A and a person B are in the same physical location and after learner A is authenticated, then person B completes the learning activities for them. Additionally, physiological authentication techniques create a low level of user experience as they require users to explicitly engage and enter authentication information (i.e. explicit authentication) through sensor activation (and they can also engender privacy concerns with the biological sample collection [10]).

Considering existing authentication solutions, continuous implicit authentication was proposed to authenticate a user continuously without interrupting an activity that the user is engaged in [8] and [9]. Implicit authentication does not require explicit user actions as it is executed as a background (non-interactive) task whilst it unobtrusively builds a user behaviour profile through sensors embedded in the authentication device [13]. It is considered as a promising authentication method with recent, increasing scrutiny as a method to enhance the usability of an authentication system [8], [9], [10], [14]. Implicit authentication has, however, the potential for poor authentication performance in practical applications as the performance tends to be impacted by associated environmental conditions [9], [15]. This leads to research interests in the study of context-aware implicit authentication systems — such systems will dynamically adapt authentication outcomes to include the contextual information such as environmental lighting and sound conditions, motion, body posture, body gesture, etc. [9].

Despite the great potential of a context-aware continuous implicit authentication mechanism, implicit authentication has not been widely applied throughout the entirety of an online learning environment, although some studies and commercial sectors have investigated its possibility for online invigilation during exam sessions [4], [6], [16], [17]. There are several studies where intensive reviews and surveys are performed to investigate online learning systems as a whole [1], [18], or they are focused on online exams [4]. Furthermore, there are few attempts to analyse the authentication perspective in online exams [19] or online learning platforms [6]. While these works provide valuable insights on authentication in online learning environments, they are not concerned with unobtrusive authentication of users considering the potential of contextual changes in online learning environments. There is a lack of studies that systematically analyse and summarise the current state of context-aware continuous implicit authentication applied in online learning environments in the literature to the best of our knowledge. Therefore, this paper sets out to systematically review context-aware continuous implicit authentication in online learning environment with the further aim to reveal the gaps in the literature covering the most up-to-date mechanisms. It establishes a research roadmap to foster advances in the field and to influence real-world implementation. The contributions of this article are:

1. The provision of a detailed analysis of the most up-to-date academic literature about context-aware continuous authentication approaches in online learning environments;
2. identification and discussion of current research challenges and limitations;
3. suggestions for future research directions through the identification of gaps in current research.

The rest of the article is organised as follows. First, the paper introduces relevant context-aware continuous implicit authentication concepts in Section II to aid with interpretation of the survey methodology described in Section III. Section IV analyses and summarises the design of the continuous implicit authentication systems found in the literature. Section V discusses the gaps identified through analysis to provide a roadmap for future research. The paper closes with a conclusion in Section VI.

II. CONTEXT-AWARE CONTINUOUS IMPLICIT AUTHENTICATION SYSTEMS

A. THE NEEDS OF A CONTEXT-AWARE CONTINUOUS IMPLICIT AUTHENTICATION SYSTEM

In online learning environments, the system should ensure that the learner who is indeed enrolled in the course is the actual individual who completes all course activities [6], [7]. Although there are various user authentication approaches applied in online learning environments, it is still susceptible to identity misuse.

Identity misuse occurs when the learner actively gives access to their account to someone else, or their account is accessed by unauthorised parties who have attacked the authentication process (typically via the use of stolen credentials) [20]. The former case has already been described as a form of academic misconduct [20]. The latter misuse occurs when password-based authentication techniques are used through attack methods such as shoulder-surfing attacks, touchscreen smudge attacks, hash-lookups in pre-computed rainbow tables and brute-force approaches using heuristics and extensive dictionaries [8], [9], [10] are used. By their very nature, online learning environments allow students to access the system remotely. The hosting educational institution has no control over remote students, and this places an added essential requirement on the learning management system to ensure the learner is a legitimate registrant on the system, especially when assessments are concerned [4], [20].

Compared to password-based authentication, biometric techniques such as face or keystroke recognition can reduce the issues of credential sharing and attacks (e.g. shoulder-surfing attacks) while achieving high authentication accuracy [3], [4]. Although biometric systems represent a robust method to authenticate users, challenges have been reported. As demonstrated in previous studies, some biometric features can change over time (for example, through ageing), and environmental conditions may also significantly influence the quality of the captured data (such as illumination, noise, and even pose). As a result, the biometric sample used to authenticate a user may no longer match the reference biometric features of the enrolled user [9], [11], [21], [22]. Samples collected during the user enrolment phase of authentication may not be representative for all possible conditions that may be encountered during the recognition phases. A simple physical change such as the distance between the sample capture device (like a camera) and a user can vary between the enrolment and recognition phases —which then highlights the need for a normalisation process of the data to ameliorate such variances. Another reason previously mentioned is due to physiological changes related to time [22], [23]. Physiological characteristics (e.g., face) are altered over time due to factors like wrinkles, injury, weight loss and gain. Sometimes illness or related treatment may impact on speech and behaviour: for example, a broken ankle will severely alter a user's gait, a broken nose may alter the facial geometry. In short, intra-class variability can decrease the authentication performance of the user in the system [9], [24].

There is a possibility of identity impersonation after the initial login phase since such authentication occurs only at login time [12], [25], [26]. Additionally, some biometric techniques require users' explicit engagement to provide authentication information through sensors; therefore, the level of user experience may reduce as a user requires active engagement for authentication [10].

B. THE DEFINITION OF A CONTEXT-AWARE CONTINUOUS IMPLICIT AUTHENTICATION SYSTEM

A context-aware continuous implicit authentication system has three key characteristics:

1. Context-awareness: the authentication system takes into account contextual data to adapt its operations [27]. The context, — also known as contextual data — is considered to be any information that may affect the authentication process (such as environmental conditions, operative conditions, type of usage, etc. [9]). An awareness of context allows the authentication system to adapt accordingly, e.g., by examining the operational environment and subsequently considering the best approach to react to changes in the environment. An example might be visible wavelength images sampled under low light levels to authenticate a physical feature may cause another authentication factor to be used instead. Related studies have proven the importance of considering contextual data in improving the authentication performance [9], [24], [28], [29], [30].
2. Continuity: the system has the ability to monitor a user's identity continuously during sessional use of the accessing device(s) to avoid issues arising from one-time authentication.
3. Non-intrusiveness: the system uses implicit authentication (IA) methods to authenticate a user without interrupting user-device interactions or requiring explicit participation during the authentication process [31]. IA harvests data about the user unobtrusively as a background task and it samples authentication data at regular and potentially short intervals (approaching continuous sampling) without requiring dedicated user action [31], [32], [33]. In general, IA does not rely on explicit input (e.g. PIN, Password, fingerprint, etc.) to authenticate a user but it closely refers to the behavioural record of the user [34]. The behavioural record should contain distinctive and measurable patterns of device usage that can be sampled without requiring deliberate user actions [28], [34].

This paper defines a context-aware continuous implicit authentication system as *a system that authenticates users with an unobtrusive approach that can modify its process and/or structure based on contextual data to improve authentication accuracy and performance.*

III. METHODOLOGY

The main objective of the study is to investigate the field of context-aware continuous implicit authentication systems in online learning to identify the knowledge gaps and the direction to advance research. Therefore, the study uses a systematic literature review method, which is a structured way to synthesise the knowledge available from primary studies in the research field [35].

The guiding research question is "*How are authentication systems designed and implemented in online learning platforms to authenticate a user unobtrusively and continuously whilst considering contextual information?*". The paper analyses the proposed system based on the research categories below:

1. Authenticator: what are the resources used to authenticate users?
2. Authentication process: what is the purpose of the authentication process?
3. Machine learning techniques: what are the machine learning techniques used in the authentication process?
4. Contextual information: what contextual information is considered in the system and how does the system change its reactions based on the contextual information?

This paper uses the search phrases "continuous context-aware implicit authentication", "continuous adaptive implicit authentication" and "continuous risk-aware implicit authentication". The discovered literature is then filtered through the specific scope: online learning or e-learning. Based on the search terms, after removing duplicates, we obtain a set of 1,766 research papers that were published from 2017 through to 2021. The following exclusion criteria are applied in order to increase the relevance of the papers selected for this study.

Documents were excluded if:

1. The publication format is other than peer-reviewed academic journal or conference paper;
2. The paper could not be retrieved using ACM digital library, IEEE explore, ScienceDirect, Scopus, or Web of Science;
3. The publication language was not English;
4. Another paper by the same authors supersedes the work, in which case the most complete (recent) work was considered;
5. It is a short paper/poster/review paper;
6. The focus is not on the design of continuous context-aware implicit authentication systems in online learning; or
7. The approach is described through non-specific generalities and not enough details were provided that addressed the research questions.

A final corpus of 17 papers was selected for a detailed review. Each paper was reviewed based on the research categories defined above. The literature is then examined to identify gaps and challenges to provide a roadmap for future research possibilities.

IV. ANALYSIS AND RESULTS

The corpus is sub-categorised according to the scope of authentication: 1) authentication for online learning platforms (OLP) to access learning materials and learning activities, 2) for online exams only, and 3) for virtual laboratory (VL). For most studies, authentication and invigilation of online exams (12 out of 17 papers) are the target area where proposals are made to use continuous authentication that considers contextual information in order to improve authentication performance. It is also observed the increase in the number of publications after COVID-19 outbreak even though research apparently decreased between 2017 and 2018 (Figure 1). It can be interpreted that there is an increase in the interest on how to secure online learning platforms due to the fast, forced transition to learning online.

A. AUTHENTICATORS

Authenticators are the managed resources used in an authentication system as a main factor to acquire user identity verification information. Authenticators are widely categorised into three categories as biometric, knowledge-based and possession based. The usage of authenticators implemented in this work, however, is divided into two categories: biometric based and knowledge based (Table 1). It is observed that there was no published use of possession-based authenticators for authentication in online learning environments.

The flexibility of authentication systems can be improved by adding diverse sets of authenticators for different scenarios [47]. Face and keystroke dynamic authenticators are supported by the majority of the surveyed works while other features (e.g.., fingerprint, mouse movement, speech, etc.) are less common authenticators (Figure 2). The implication is that samples of face and keystroke dynamics can be easily collected using standard computing devices without any additional hardware [12], [26]. In addition, face and keystroke dynamics can be captured automatically and continuously without interrupting a user's interactions with the accessing device during the entire online interaction session [12], [16]. One paper that uses both keystroke dynamics and passwords as authenticators applies the keystroke dynamics as an additional assurance for a password [45]. For example, a password is required from the user as a first factor of authentication, and keystroke dynamics of the password input itself is used as an additional assurance of authentication behind the scenes. Behavioural characteristics, in particular, are included more frequently in authentication rather than physiological traits and knowledge-based authenticators. The reason for this choice is that behavioural traits are good candidates for

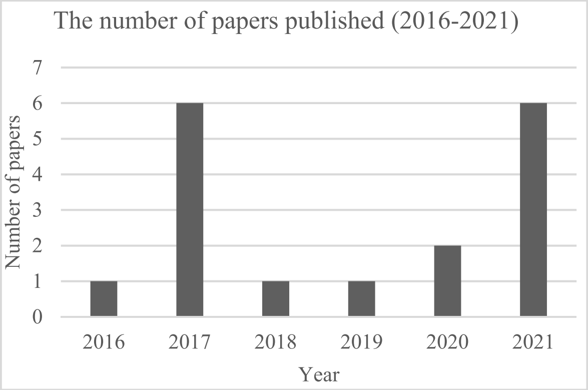


FIGURE 1. The number of candidate papers published in each year from 2016 to 2021.

TABLE 1. Overview of authenticators applied in authentication system.

Scope	Paper	Biometrics										K
		F	Fi	M	K	T	W	V	S	G	B	P
Exam	[12]	x		x	x							
	[36]				x							
	[37]	x	x							x		x
	[38]	x					x		x	x		x
	[39]										x	x
	[40]											
	[41]	x			x							
	[23]	x										
	[42]				x							
	[25]	x	x		x							
	[43]	x								x		
	[44]				x							
OLP	[21]				x							
	[26]	x		x	x	x		x				
	[45]				x							x
	[16]	x			x				x		x	
VL	[46]	x										

Legend: K. = Knowledge-based; F = Face; Fi = Fingerprint; M = Mouse Dynamics; K = Keystroke Dynamics; T = Touch; W = Writing Style (text); V = Voice; S = Speech; G = Gaze (Eye movement); B = Behaviour Profile; P = Password.

continuous authentication purposes compared to physiological characteristics, since the user can be implicitly detected without requiring explicit interaction.

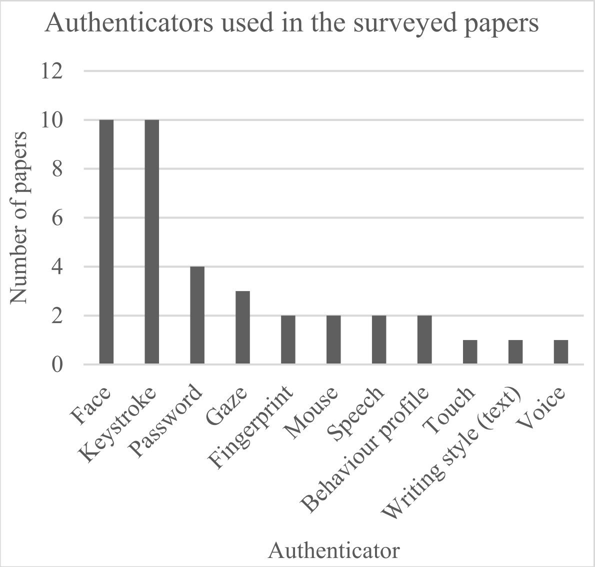


FIGURE 2. The frequency of authenticators used in the survey paper.

B. AUTHENTICATION PROCESS

The authentication process can be categorised into two sub-processes based on purpose: i) identity assurance and ii) authorship assurance for fraud detection. Authentication verifies a user's credentials using the system's defined authenticator to ensure that the users are who they 'say' they are. The identity assurance ensures the identity of the learners in online learning environments while authorship assurance is concerned with the identity of the creator of user-generated content in order to ensure that the learning outcomes are achieved by the authenticated user [40], [48], [49]. Table 2 provides the overview of the authentication process in the surveyed papers and what authenticators are used for identity assurance and authorship assurance.

1) IDENTITY ASSURANCE

Identity assurance is the first and primary step in the authentication process for online learning [48]. It is important to have an effective identification strategy to track the user's activity and progress in online learning environments [40], [48]. Identity assurance starts with the pre-registration of a user through the acquisition and recording of a user's information using the authenticator. Regardless of the type of authenticator used, an accurate identity template should be created prior to the identity assurance process. The authentication system then compares the real-time collected sample to the template that has been generated during the enrolment process [48].

It is observed that the majority of the surveyed papers investigate the use of the face as a main authenticator for identity assurance. This may be because: i) facial recognition has shown a high accuracy rate consistently in the literature facial recognition has shown a high accuracy rate consistently in the literature [16], [23], [26]; ii) real-time facial recognition can leverage commonly integrated webcams in the authenticating device [46]; and/or iii) a face cannot be lost or forgotten (ignoring trauma and/or deliberate masquerading) [40].

TABLE 2. Overview of the authentication process detailed in the surveyed papers with the use of authenticators in each process.

Scope	Paper	Identity assurance	Authorship assurance (Fraud detection)
Exam	[12]	Face, Mouse, Keystroke	
	[36]	Keystroke	
	[37]	Password, Fingerprint	Eye-Gaze
	[38]	Face	Computer monitoring, Text, Speech, Eye-Gaze
	[39]	Password, Behavioural profile	Behaviour analysis
	[40]	Face, Voice	Writing/Plagiarism detection
	[41]	Face, Keystroke	Face, Keystroke
	[23]	Face	Face
	[42]	Keystroke	Keystroke
	[25]	Face, Fingerprint, Keystroke	
	[43]	Face	Eye-Gaze
	[44]	Keystroke	
OLP	[21]	Keystroke	Keystroke
	[26]	Face, Mouse, Keystroke, Touch, Voice	
	[45]	Keystroke	Keystroke
	[16]	Face, Keystroke, Voice	Behaviour analysis, Computer monitoring
VL	[46]	Face	Face tracking

Among the behavioural authenticators, keystroke dynamics is the most popular characteristic used for identity assurance. The reasons for this choice are: i) it can be used with password for additional assurance; ii) it does not require additional hardware; and iii) it can collect the data passively. Continuous face and keystroke dynamic authentication verify a user during an entire session which can detect fraud/cheating as an alert can be raised if a user has been replaced by other individual [12], [14], [16], [25], [26], [36], [44], [45], [46]. The surveyed papers use both static and free-text keystroke dynamics to verify a student's authenticity by collecting keystroke information during the overall online learning process, which includes factors such as how the user manipulates text, how they capitalize letters and the position of the control keys used [45].

2) AUTHORSHIP ASSURANCE

Authorship assurance is another critical factor in the learners' authentication process [48]. Authorship assurance is more focused on verifying the user activity continuously; therefore, it is observed that the authenticator used for authorship assurance is chosen depending on whether it can monitor a user's continuous activities. Authorship assurance can be confirmed though cheating behaviour detection.

Cheating behaviours include: 1) the presence of alternative or additional people in an assessment session for an individual [16], [38], [43]; 2) abnormal eye movement indicating the user is looking elsewhere for the answer [37], [38], [43]; and 3) the use of non-permitted devices/sources [16], [38], [43].

Vision and audio technologies which use face, speech, or voice detection are widely used to detect whether there are multiple people present during the session. Audio detection determines whether there are any unnecessary conversations occurring [16], while face recognition is used to detect 1) only one person is in view, whether this person is the person who was authenticated at the beginning of the session [16], [23], [41] and/or 2) if multiple faces are detected [16], [38].

Tracking eye movement (including gaze monitoring) is the most popular method to detect cheating behaviour during online exams [37], [38], [43]. Although an abnormal gaze does not directly mean the confirmation of cheating behaviour, it is an important clue to suggest the possible subsequent cheating actions [38]. Two studies monitor and detect abnormal gazes of the user along with face recognition [38], [43]; while Bawarith et al. [37] continuously senses eye tracking without face recognition.

The use of non-permitted devices/sources are detected through computer monitoring or device detection using images captured from web cameras [16], [38]. The activity within the devices of the users who are doing the assessment activity is also monitored [16]. The most common method of computer monitoring is observing active windows running in the system [16], [38]. Apart from the detection of active windows, Labayen et al. [16] explored additional tools to monitor the computer's activity including the detection of the running process, peripheral devices connected to the computer, browser history, screenshots, device information such as IP address, operating system, etc. It is expected that including information associated with various monitoring techniques in the analysis of the authenticity of the student may provide a more comprehensive authentication and invigilating process [16]. Texting/messaging and phone detection are performed through a camera to prevent cheating arising from reading non-permitted text or phone usage [38].

C. MACHINE LEARNING IN THE AUTHENTICATION PROCESS

Machine learning (ML) is a branch of artificial intelligence that enables systems to recognise patterns in data and to predict outcomes using a mixture of algorithms and statistical models without explicit instructions [50]. ML has been widely applied to construct a verification model for authentication by building a mathematical model-based training dataset — predictions (regressions), classification and pattern recognition. The various ML techniques are utilised to analyse videos, images, sounds, etc. [24], [36], [38], [42]. This section discusses the different types of machine learning techniques used for feature detection and verification in authentication systems.

1) FEATURE DETECTION

OpenCV [51] is an open-source library of computer vision and object detection techniques, which is widely applied to face recognition. It has been used for face recognition systems to save development time with the Principle Component Analysis (PCA) method [46]. However, OpenCV's existing face tracking algorithm does not scale and/or perform well in real-world environments for continuous authentication purposes [12]. Traoré et al. [12] modified the tracking algorithm to work with individual face frames sent to the system for recognition without requiring a specific number of frames before decisions can be made.

YOLO (You Only Look Once) [52] is a neural network used to detect objects in real-time. It has been widely applied for face detection in literature due to its speed and convenience — it scans an image only once for object detection while other systems need several analytical passes on an image for detection [43]. YOLO with a Convolutional Neural Network (CNN) feature extractor has been applied to detect faces during an exam [43], while Ganidisastra and Bandung [23] combined two different deep learning face detection methods, Multi-Task Cascaded CNN (MTCNN) and YOLO-face, to detect the faces under various light and pose conditions.

2) VERIFICATION/CLASSIFICATION

For face verification, deep learning algorithms are a frequent method applied in authentication systems. The FaceNet model for face recognition provides high accuracy in verification and identification [23]. VGG Face [53], which uses the CNN architecture for recognition, is widely adopted in the literature since it is proven to be very effective in image recognition and classification compared to FaceNet and the DeepFace system [41], [43]. Two reviewed papers [16], [46] use different verification/classification methods for face recognition such as the Nearest Neighbour algorithm [46] or FaceBoxes methodology to optimise GPU usage [16].

For keystroke recognition, Subash and Song [42] compare the authentication accuracy with different classification algorithms: Multi-Perceptron (MLP) algorithm [54], CNN [55], Naïve Bayes (NB) [56], and Decision Tree (DT) [56] to find the best classification methods and proposed architectures in their study. The combination of CNN and Recurrent Neural Network (RNN) models has been applied to learn the personal keystroke input for continuous authentication to improve the performance of authentication accuracy [16].

Ensemble-based classification — when the system uses multiple authenticators to authenticate the user — is used as it reduces the errors in predictions in the model due to variance, bias and noise [38], [43]. One of the surveyed papers investigates four supervised classification algorithms: DT, Logistic regression, k-nearest neighbours scheme and a NB classifier for the continuous analysis of face and keystroke during the session [41].

It is observed that various machine learning techniques are applied to the system; however, there is a lack of discussion on the impact of the machine learning technique during the authentication process in terms of accuracy and efficiency. There is the trade-off between system performance and strength with the adoption of machine learning techniques for the biometric authentication system [57], however, most studies are focused on the accuracy of the authentication system while neglecting the computation complexity and latency caused by the machine learning which influences the resulting usability of the system.

D. CONTEXTUAL INFORMATION

A authentication system's behaviour may be affected through the inclusion of contextual information [9]. Such information is usually considered in attempts to improve the system performance (Table 3).

User activity is the most popular contextual information that is considered in the literature. Depending on the measured interactions between a peripheral device and the user, the system may initiate another authenticator to identify the user [12], [37]. For instance, if the user has less mouse and keyboard interactivity, the system may then initiate a face authenticator, or alternatively, when user eye-tracking monitoring fails, re-authentication may be required using fingerprints [37]. Haytom et al. [41] activates keystroke dynamics only when the input text is longer than the equivalent of one page of content; otherwise, the face is the main user-verifying authenticator. The engagement between users and online learning courses is also considered as contextual information to detect abnormal behaviour and build the student's profile [39], [42], [45]. For example, to build a more comprehensive template for keystroke dynamics, the length of words, repetition of the word and the number of words found in the student's writing are considered [21].

External conditions such as illumination or noise in the background of images have a significant impact on the recognition performance of physiological biometric traits (e.g., face) since it impacts on the quality of the data collected from the user. Therefore, studies take into account external conditions so that the system can adjust its parameters during the recognition process [16], [23], [41], but the approaches on how to use external condition contextual information in the recognition process differ. Since the quality of the facial images is a crucial factor which determines the accuracy of the recognition performance, if the image quality is too low it is discarded [41]. Different body movements or poses also influence the authentication performance. Hence, Ganidisastra and Bandung [23] collect the face images with various poses and lightning conditions during the registration phases, then update the face data during the online lecture session using incremental training, which adds new data to the training dataset. Interestingly, human-interruption is proposed by Labayen et al. [16] when the quality of vision and audio do not meet the required threshold(s).

Regardless of the type of biometric authenticators, biometrics change over time due to various factors such as physical ageing, emotional status, etc. Therefore, updating the reference of the biometric traits over time has been suggested so that the most accurate authentication based on contemporary biometric features can be achieved [36], [46]. The emotion of the user is also considered during the collection of data by relating each sampled feature to a user's emotional status [36], [43].

Fenu et al. [26] suggested a system which integrates with five biometric subsystems by applying a reliability measure. The reliability measure considers the context where the matching score for the classification is computed rather than just selecting the score based on the quality of input data. The reliability of the system is calculated considering the device that the user is using and the interaction between the device and the user. It helps to identify which device that is coupled to the system can achieve more accurate authentication of the user, which can then enable suggestions as to which device should be used for example, for online exams.

TABLE 3. Overview of the contextual information considered in the literature to improve authentication performance during sessions.

Scope	Paper	E	U	B	T	Em	SB	TR
Exam	[12]		x					
	[36]				x	x		
	[37]		x					
	[38]		x	x			x	
	[39]		x					
	[40]							
	[41]	x	x					
	[23]	x		x				
	[42]		x					
	[25]						x	
	[43]					x		
	[44]				x			
OLP	[21]		x					
	[26]		x					x
	[45]		x					
	[16]	x	x					
VL	[46]				x			

Legend: E = External Conditions (e.g. light, noise, etc.); U = User activity; B = Body movement/Pose; T = Time; Em = Emotion; SB = Soft Biometrics (clothes, gender, skin colour, etc.); TR = Technical Resources

E. EVALUATION APPROACH

The evaluation of authentication systems is important to ensure the feasibility of the system as a safeguard of online learning environments. Various evaluation approaches have been performed in the literature to provide assurances of the online learning environment's security trustworthiness (Table 4).

TABLE 4. Overview of the type of datasets used in system evaluation.

Scope	Paper	Type of dataset	Dataset
Exam	[12]	Public and Private	Public: AT&T Face Database, Yale Face Database, Yale Face Database B Private: 11 participants
	[36]	Private	8 participants
	[37]	Private	30 participants
	[38]	Private	24 participants
	[39]	N/A	MATLAB simulation
	[40]	Private	3500 participants
	[41]	Private	30 participants
	[23]	Private	4 participants
	[42]	Public	CMU benchmark
	[25]	Public	ORL database Yale face database FASSEG database FVC 2004 Keystroke: : Killourhy and Maxion [58]
	[43]	Private	4 participants
	[44]	Public and Private	Public: Data from the articles : Killourhy and Maxion [58], Sun, Ceker and Upadhyaya [59],[60] Private: 27 participants
	[21]	Private	60 participants
OLP	[26]	-	-
	[45]	Private	8 participants
	[16]	Private	350 participants
VL	[46]	Private	30 participants

1) DATASET

When the system requires continuous authentication of a user while considering the context of the environment, the dataset used in the system is expected to contain several samples per user captured over time under uncontrolled circumstances [22]. One study — [12] — is an exception as it uses both public and private data. But otherwise the majority of the papers reviewed collect data from participants to evaluate the system instead of using available public datasets (Figure 3). Due to the limited availability of suitable public datasets for evaluations of authentication systems for online learning environments it is difficult to generalize these evaluations for comparison purposes [38].

The datasets collected by the surveyed researchers range from 4 to 3,500 participants. Other than the TeSLA project [40], which is a collaboration between seven universities, most of the reviewed papers have fewer than 30 participants — the small number of participants may create doubt in the validation results of the reviewed authentication systems.

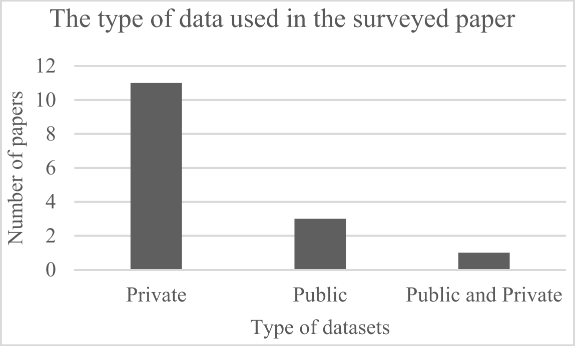


FIGURE 3. The type of datasets used in the surveyed papers to evaluate the proposed system.

Some of the data are collected in controlled environments such as typing a pre-defined sentence to collect keystroke data [36] or typing a password [45]. Alternatively, there are attempts to collect dynamic datasets by scheduling different experimental sessions to justify the use of a context-aware continuous authentication system.

When detecting cheating behaviour, participants are asked to actively cheat through various activities while completing an exam without any instructions on what cheating behaviour to perform or how to perform it [37], [38].

Zamfiroiu et al. [45] collect two types of keystroke datasets with different usage purposes — static text from entering a password and dynamic text while sitting an exam. The static dataset which is acquired through typing a password is then utilised for one-time authentication to access an exam session while keystroke data collected from dynamically entered text is used to verify the student's identity after taking an exam.

Different experiments are undertaken to collect more dynamic data to prove that the authentication accuracy has improved in their studies [16], [23], [41]. The external conditions (lighting, occlusion and background noise) and user activity (distance between the webcam and the user, pose, and expression) were manipulated while collecting the face dataset to acquire a variety of face images [23], [41] Ganidisastra and Bandung [23] collect different facial images for participants by varying pose, lighting, occlusion, expression and distance between the camera and the participant while Haytom et al. [41] acquire different biometric data (face and keystroke) under three different experimental sessions with different purposes. The first session is targeted to collect a variety of facial images in both controlled and uncontrolled environments through the variation of the light, pose and background images. Keystroke data is acquired in the second session for a day without pre-defined text. The third experiment is focused on the collection of fraudulent data with audio, image and keystroke dynamics data. Instead of setting up different environments to collect the specific dataset, each experiment is held with different assessment activities involving different e-learning institutions in different countries [16]. This enables the collection of large datasets reflecting real-world activities as they occur on the learning platform, and as a consequence a more complete experience of the biometric authentication and invigilating systems is obtained.

Different public datasets are also utilised to evaluate some of the systems proposed in literature since a number of public datasets are available for face and keystroke dynamics [12], [25], [42], [44]. With public datasets, a system can be evaluated with the large number of datasets to explore the feasibility and effectiveness of the authentication framework [44]. As a general principle, evaluation results are more statistically significant and trustworthy if a higher number of users are engaged for the performance experiments [22]. It is also important, however, to have a comprehensive dataset which has varied environmental and behavioural contexts to effectively evaluate context-aware systems [11], [22].

2) EVALUATION METRICS

Different evaluation metrics have been applied in the literature to assess the recognition performance of context-aware continuous implicit authentication systems. The evaluation metrics are categorized into 1) technical and 2) user evaluation (Table 5).

a: TECHNICAL EVALUATION

Technical evaluation involves monitoring the error rates of the authentication system in order to improve the recognition performance [22]. The most popular evaluation metric applied is a matrix based on the confusion matrix (known as the contingency table, —Table 6) which contains four cells, and using the confusion matrix, four different aspects of performance can be measured [12], [23], [25], [36], [37], [38], [42], [43], [46].

Several metrics used to assess the recognition performance of biometric systems are also common to the evaluation of other authentication systems such as False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER). FAR calculates the ratio of imposter attempts that were wrongly classified as an authentic user by considering the rate where the system fails to obtain a biometric sample. In contrast, FRR considers the rate of authentic user attempts that were incorrectly classified as an imposter with the possibility of a failure of acquiring a biometric sample [22]. The EER can be calculated through finding the points where both FAR and FRR are equal — the lower the EER value, the higher the accuracy of the biometric authentication system.

Since some of studies are focused on invigilation as well as authentication, other approaches have been used to evaluate how the system detects cheating [38], [44]. Average monitoring cycles to catch cheaters (CTC) and average false rejection counts (FRC) are calculated to evaluate how effectively the keystroke continuous authentication system detected cheaters [44]. Atoum et al. [38] evaluated a proposed system using two different approaches: a segment-based metric and an instant based metric using FAR and True Detection Rate (TDR) (Figure 4).

TABLE 5. Summary of evaluation approaches and indicators used in surveyed papers.

	Approach	Indicator	# of papers	Paper
Technical evaluation	Confusion matrix based	Accuracy	9	[12, 23, 25, 36-38, 42, 43, 46]
		Precision	4	[16, 25, 37, 42]
		Sensitivity (Recall, TPR)	4	[16, 25, 37, 42]
		F-measure	3	[25, 37, 42]
		Specificity (TNR)	2	[25, 37]
	Common in biometric systems	FAR (FPR)	7	[21, 25, 38, 41, 42, 44, 45]
		FRR (FNR)	5	[21, 25, 41, 44, 45]
		EER	2	[41, 44]
	Cheating-focused	TDR	1	[38]
		CTC/FRC	1	[44]
	Others	Kappa statistics	1	[42]
		Authentication level	1	[39]
	Efficiency	Time	1	[23]
		Disk usage	1	[23]
		Computation cost	1	[38]
	Effectiveness	Long-term stability	1	[26]
		Device/interaction agnosticism	1	[26]
	Usability (Disturbance)		1	[26]
	Security		1	[26]
User evaluation		User Experience	3	[16, 40, 46]

Legend: TPR (True Positive Rate); FAR (False Acceptance Rate); FPR (False Positive Rate); FRR (False Rejection Rate); FNR (False Negative Rate); EER (Equal Error Rate); TDR (True Detection Rate); CTC (Cycles to catch cheaters); FRC (False Rejection Count)

TABLE 6. A confusion matrix used for biometric authentication systems with the formulas of accuracy, sensitivity, specificity and F1- measure.

	Authorised user (Positive)	Unauthorised user (Negative)
Grant Access (Positive)	True Positives (TP)	False Positives (FP)
Deny Access (Negative)	False Negatives (FN)	True Negatives (TN)

Accuracy = (TP + TN) / (TP+TN+FP+FN)
Sensitivity (True Positive Rate (TPR), Recall) = TP / (TP+FN)
Specificity (True Negative Rate (TNR) = TN / (TN+FP)
F1-measure = 2TP / (2TP + FP +FN)

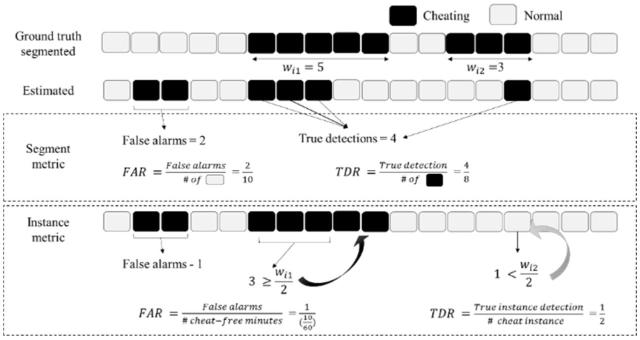

Cheating
Normal
Ground truth segmented
$w_{i1} = 5$
$w_{i2} = 3$
Estimated
Segment metric
False alarms = 2
True detections = 4
$FAR = \frac{False\ alarms}{\#\ of\ ☐} = \frac{2}{10}$
$TDR = \frac{True\ detection}{\#\ of\ ■} = \frac{4}{8}$
Instance metric
False alarms - 1
$3 \geq \frac{w_{i1}}{2}$
$1 < \frac{w_{i2}}{2}$
$FAR = \frac{False\ alarms}{\#\ cheat\text{-}free\ minutes} = \frac{1}{(\frac{10}{60})}$
$TDR = \frac{True\ instance\ detection}{\#\ cheat\ instance} = \frac{1}{2}$

FIGURE 4. The example of segment and instance-based metrics used in Atoum et al. (2017).

Most of the reviewed papers provide a quantitative analysis to evaluate the system's technical performance, however, a preliminary qualitative comparison between a proposed system and other existing solutions was conducted by Fenu et al. [26] identifying six dimensions: security, usability, efficiency, long-term stability, device-agnosticism and interaction-agnosticism. The study elaborates how the proposed system can alleviate the challenges captured in other existing solutions, for example, how the proposed system is designed to work across various types of devices or how much the system disturbs a student's activity to ask specific interaction for recognition purposes.

b: USER EVALUATION

User evaluation qualitatively measures a user's overall perception and acceptance of the system and it is one of the most important factors to ensure the system's feasibility under real-world deployments [16]. Investigating user experience on a proposed system using a participation/post-participation survey is the most popular method in the literature that was used to evaluate the suitability of a system or the attitudes of the users towards a proposed system [16], [40], [46]. While Zhangetal. [46] and the TeLSA project [40], [61] focus solely on the students' attitudes, the students' and the teachers' perceptions are considered in Labayen et al. [16]. The latter's survey questions are formulated to evaluate the users' experiences of using the online learning system with the proposed authentication system, such as the acceptance of using the system (i.e., how much the users are in favour of using the system), convenience of undertaking the required task with the proposed system, or the perception of using the system in an online learning environment.

V. DISCUSSION AND FINDING

This systematic review has investigated the current status of the research literature on context-aware continuous authentication applied in online learning environments. The issues of how to maintain and integrate academic integrity in online learning environments have been the major considerations for more than decade [4], [6]. Nevertheless, the possibility of academic misconduct exists in face-to-face learning environments as well, and the absence of face-to-face interactions between instructors and students in online learning environments has enforced new means for academic misconduct and dishonesty to develop.

To combat academic dishonesty and misconduct, an online learning environment should 1) verify the identities of online students, 2) ensure that there is no cheating involved during online assessment activities including exams and 3) assess the performance sufficiently [26]. In the reviewed literature, most solutions are designed to authenticate and invigilate students during online exams (see Figure 2) without considering other aspects of the learning process and experience. Academic dishonesty and misconduct occur not only during online exams, but also, for example, through course participants sharing identities. Therefore, there is a requirement to explore how to authenticate users to establish trust in the authorship of the work during, and after, learning sessions [16], [26], [45].

A. AUTHENTICATOR DIVERSITY CHALLENGES

Using biometrics in a continuous context requires a system to constantly collect and measure biometric traits during a session [11]. Hence such systems must satisfy the following criteria: performance (recognition accuracy and speed) and collectability (features are measurable and are able to be represented in digital formats). Collectability relates to the usability of the systems as it requires a minimum threshold amount of user involvement to acquire the data. In cases where a user may not be willing to cooperate in the provision of the required biometric data, certain biometric traits (e.g., fingerprints) are simply unsuitable for continuous authentication systems even though they are successful in non-continuous authentication systems.

Thus, face and keystroke dynamics are appropriate authenticators in online learning environments since users usually do not significantly move in relation to their position with respect to the camera [11] and those features can be captured passively without interrupting users' activity during the session [11], [26], [41], [46].

There are various biometric features that are increasingly being applied to cater for a multitude of different (and increasingly ubiquitous) devices such as touch, and biomedical signals. By contrast, face (or face-related features such as iris analysis) and keystroke dynamics are the dominant biometric features used in online learning environments — with the assumption that a user will only use a laptop or desktop system. Since there are various devices available to connect to online learning platforms, however, such as smartphones, tablets, etc., a user may utilise multiple devices to perform online learning activities including exams. In these cases, the user's face may not be visible using mobile devices such as a mobile phone as the user will move their position frequently [11] and video processing may impact energy consumption [62]. Therefore, an exploration of the dynamic use of authenticators is needed to cover other types of user interaction in online learning environments. This leads to the investigation of various machine learning techniques applied in the authentication process including feature extractions and classifications in relation to chosen biometric features so that the authentication system can leverage different devices without any performance or accuracy hurdles ensuring continuous recognition.

B. TEMPLATE AGEING

Due to challenges associated with the use of biometric authenticators such as template ageing or intra-class variation, considering additional contextual information has been proposed to improve the recognition performance. Context-aware continuous authentication systems include dynamic operating environments in the literature in relation to the biometric authenticator they have chosen. Regardless of the type of authenticator used, all the included studies have considered a passive context-awareness approach — the system constantly observes the environment or user activity in order to offer the appropriate options to the user [63]. The system monitors users' activities in online learning platforms to utilise the best authenticator to identify the user without interrupting their activities. For example, if face recognition is not available or it is not suitable due to the system assigning method with a low confidence score due to poor image quality, then keystroke dynamic may be chosen if a user's typing is detected instead. Along with physiological traits, the external environment (e.g., illumination) has been considered since physiological characteristics are more sensitive to the surrounding environment [16], [23], [41]. Therefore, most studies are more focused on how to tune the parameters or structure in the authentication process considering the contextual information given with acquired data. Physiological characteristics, however, also can be changed due to physical ageing or injury (e.g. scars on face due to the injury) causing template ageing of biometric references. Although some studies consider template adaptation to minimise the impact of change in a biometric measure over time [36], [46], they lack an investigation into template adaptation which includes determining when and what thresholds trigger an adaptation process to update the biometric data, or how to change the biometric data in detail.

C. SECURITY AND PRIVACY CHALLENGES

One of the most common security attacks toward biometric authentication systems is a presentation attack to cheat the authentication process with something that would otherwise be an authentic identity. A face presentation attack happens when the user presents a printed or digital photograph of the claimed identity, or through video play back on an electronic screen [64]. Voice presentation attacks concern replaying the recorded speech of the claimed identity or using voice software to generate the voice of the claimed identity from text [65]. Only limited studies consider how to protect the biometric authentication system from these types of attacks using standard encryption and digital certificates [41]. It is observed that most surveyed papers neglect privacy issues associated with the use of biometric traits even though the privacy of the collection of biometric traits has been a major concern for a considerable time [14], [41], [66]. Hence, there is a requirement to investigate how to secure the biometric authentication systems from privacy and security attacks.

D. EVALUATION CHALLENGES

Experimental studies in most of the reviewed literature have been conducted in small- to medium-sized datasets ranging from 4 to 350 participants (see Table 4). Even though the systems are evaluated under unconstrained environments to reflect real-world interactions, the number of users of the system in online learning environments is typically much higher. The lack of evaluation with a large-scale scenario is a current challenge. With a large-scale evaluation, new questions could be addressed such as whether the performance of the authentication system scales efficiently with the system load associated with activity (e.g., taking exams, online learning activities, etc.). This finding will give insights on how a proposed system can integrate with the current online learning platform offering the same or a higher quality of service.

The majority of studies are focused on the evaluation of a system's recognition accuracy based on the confusion matrix and/or common matrix in biometric systems (see Table 5). As there is no standard to evaluate the accuracy of context-aware continuous authentication systems, it is difficult to determine whether the indicators used for recognition accuracy provides reliable results. Since authentication in online learning environments involves two phases with different purposes — identity verification and authorship assurance — there is a need to explore whether applying the same criteria is appropriate to evaluate a system or whether the evaluation approach commonly used in authentication systems can provide reliable results.

Usability is a key aspect of secure system design as it is related to favourable user acceptance [47]. Despite its importance, few studies on context-aware continuous authentication include usability studies which include effectiveness, efficiency, and user acceptance of the system [16], [23], [26], [40], [46]. Therefore, there is a need for future studies to explore user acceptance and the usability of the system that considers different devices (e.g., mobile devices).

VI. CONCLUSION

Context-aware continuous implicit authentication can verify the identity of individuals continuously, considering contextual information given, and can do so passively, without interrupting users. The aim of this study is to provide a review of context-aware continuous implicit authentication systems applied in online learning environments, covering aspects such as authenticators, the authentication process, contextual information, and evaluation approaches. To the best of our knowledge, this is the most up-to-date review of context-aware continuous implicit authentication in online learning environments. This paper has provided a review of works in authentication in online learning platforms by categorising systems based on their targeted scope so that the reader can readily perform comparisons. The scope has been divided into online exams, online learning platforms and virtual laboratories with detailed analysis of the design of context-aware continuous implicit authentication systems provided.

A discussion of the systems including their evaluation approach is a key aspect of this article. Based on the discussion, this paper concludes that there are several gaps in the literature: authentication scope, authenticator diversity, template ageing, and system evaluation. We believe that this paper can assist in the understanding of context-aware implicit authentication systems in online learning environments and foster research advances on the topic.

REFERENCES

[1] C. McCoy, A. Yu, and S. Ramazanova, "An author co-citation analysis: Examining the intellectual structure of e-learning from 1981 to 2014," in *Proc. 78th ASIS'T Annu. Meeting: Inf. Sci. Impact: Res. Community*, St. Louis, MO, USA, 2015, pp. 1–3.

[2] J. Crawford, K. Butler-Henderson, J. Rudolph, B. Malkawi, M. Glowatz, R. Burton, P. Magni, and S. Lam, "COVID-19: 20 countries' higher education intra-period digital pedagogy responses," *J. Appl. Learn. Teach.*, vol. 3, no. 1, pp. 9–28, 2020.

[3] X. Zhu and C. Cao, "Secure online examination with biometric authentication and blockchain-based framework," *Math. Problems Eng.*, vol. 2021, Aug. 2021, Art. no. 5058780.

[4] A. W. Muzaffar, M. Tahir, M. W. Anwar, Q. Chaudry, S. R. Mir, and Y. Rasheed, "A systematic review of online exams solutions in E-learning: Techniques, tools, and global adoption," *IEEE Access*, vol. 9, pp. 32689–32712, 2021.

[5] D. Hond and L. Spacek, *Face Database*. Colchester, U.K.: Univ. Essex, 1997.

[6] J. Curran and K. Curran, "Biometric authentication techniques in online learning environments," in *Research Anthology on Developing Effective Online Learning Courses*. Hershey, PA, USA: IGI Global, 2021, pp. 867–879.

[7] E. R. Weippl and M. Ebner, "Security privacy challenges in e-learning 2.0," in *Proc. E-Learn: World Conf. E-Learn. Corporate, Government, Healthcare, Higher Educ.*, Las Vegas, NV, USA, 2008, pp. 1–6.

[8] M. Abuhamad, T. Abuhmed, D. Mohaisen, and D. Nyang, "AUToSen: Deep-learning-based implicit continuous authentication using smartphone sensors," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5008–5020, Feb. 2020.

[9] R. Wang and D. Tao, "Context-aware implicit authentication of smartphone users based on multi-sensor behavior," *IEEE Access*, vol. 7, pp. 119654–119667, 2019.

[10] T. Zhu, Z. Weng, Q. Song, Y. Chen, Q. Liu, Y. Chen, M. Lv, and T. Chen, "EspialCog: General, efficient and robust mobile user implicit authentication in noisy environment," *IEEE Trans. Mobile Comput.*, vol. 21, no. 2, pp. 555–572, Feb. 2022.

[11] G. Dahia, L. Jesus, and M. Pamplona Segundo, "Continuous authentication using biometrics: An advanced review," *WIREs Data Mining Knowl. Discovery*, vol. 10, no. 4, p. e1365, Jul. 2020.

[12] I. Traoré, S. Saad, B. Sayed, J. D. Ardigo, and P. M. De Faria Quinan, "Ensuring online exam integrity through continuous biometric authentication," in *Information Security Practices: Emerging Threats and Perspectives*. New York, NY, USA: Springer, 2017, pp. 73–81.

[13] Y. Yang, J. Sun, and L. Guo, "PersonaIA: A lightweight implicit authentication system based on customized user behavior selection," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 1, pp. 113–126, Jan. 2019.

[14] F. Wei, S. Zeadally, P. Vijayakumar, N. Kumar, and D. He, "An intelligent terminal based privacy-preserving multi-modal implicit authentication protocol for internet of connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3939–3951, Jul. 2021.

[15] N. Zheng, K. Bai, H. Huang, and H. Wang, "You are how you touch: User verification on smartphones via tapping behaviors," in *Proc. IEEE 22nd Int. Conf. Netw. Protocols* Oct. 2014, pp. 221–232.

[16] M. Labayen, R. Vea, J. Florez, N. Aginako, and B. Sierra, "Online Student authentication and proctoring system based on multimodal biometrics technology," *IEEE Access*, vol. 9, pp. 72398–72411, 2021.

[17] S. Arnò, A. Galassi, M. Tommasi, A. Saggino, and P. Vittorini, "State-of-the-art of commercial proctoring systems and their use in academic online exams," *Int. J. Distance Educ. Technol.*, vol. 19, no. 2, pp. 55–76, 2021.

[18] V. Chang, "Review and discussion: E-learning for academia and industry," *Int. J. Inf. Manage.*, vol. 36, no. 3, pp. 476–485, Jun. 2016.

[19] N. A. Karim and Z. Shukur, "Review of user authentication methods in online examination," *Asian J. Inf. Technol.*, vol. 14, no. 5, pp. 166–175, 2015.

[20] L. Q. Huan, D.-M. Nguyen, H.-A. Pham, and N. Huynh-Tuong, "Authentication in E-learning systems: Challenges and solutions," *Sci. Technol. Develop. J.-Eng. Technol.*, vol. 3, no. SI1, pp. SI95–SI101, Dec. 2020.

[21] A. D. Josa, E. S. Perez, and J. A. M. Moreno, "Using keystroke dynamics and context features to assess authorship in online learning environments," *Proc. 11th Int. Conf. Technol., Educ. Develop. (INTED)*, Valencia, Spain, May 2017.

[22] P. H. Pisani, A. Mhenni, R. Giot, E. Cherrier, N. Poh, A. C. P. de Leon Ferreira de Carvalho, C. Rosenberger, and N. E. B. Amara, "Adaptive biometric systems: Review and perspectives," *ACM Comput. Surv.*, vol. 52, no. 5, p. 102, 2019.

[23] A. H. S. Ganidisastra and Y. Bandung, "An incremental training on deep learning face recognition for M-learning online exam proctoring," in *Proc. IEEE Asia Pacific Conf. Wireless Mobile (APWiMob)*, Apr. 2021, pp. 213–219.

[24] W.-H. Lee and R. B. Lee, "Implicit smartphone user authentication with sensors and contextual machine learning," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2017, pp. 297–308.

[25] H. Purohit and P. K. Ajmera, "Multi-modal biometric fusion based continuous user authentication for E-proctoring using hybrid LCNN-salp swarm optimization," *Cluster Comput.*, vol. 25, no. 2, pp. 827–846, Apr. 2022.

[26] G. Fenu, M. Marras, and L. Boratto, "A multi-biometric system for continuous Student authentication in e-learning platforms," *Pattern Recognit. Lett.*, vol. 113, pp. 83–92, Oct. 2018.

[27] B. Schilit, N. Adams, and R. Want, "Context-aware computing applications," in *Proc. 1st Workshop Mobile Comput. Syst. Appl.*, Dec. 1994, pp. 85–90.

[28] C. Wu, K. He, J. Chen, R. Du, and Y. Xiang, "CaIAuth: Context-aware implicit authentication when the screen is awake," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11420–11430, Dec. 2020.

[29] W. Xu, Y. Shen, C. Luo, J. Li, W. Li, and A. Y. Zomaya, "Gait-watch: A gait-based context-aware authentication system for smart watch via sparse coding," *Ad Hoc Netw.*, vol. 107, Oct. 2020, Art. no. 102218.

[30] F. Sun, C. Mao, X. Fan, and Y. Li, "Accelerometer-based speed-adaptive gait authentication method for wearable IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 820–830, Feb. 2019.

[31] W.-H. Lee, X. Liu, Y. Shen, H. Jin, and R. B. Lee, "Secure Pick up: Implicit authentication when you start using the smartphone," in *Proc. 22nd ACM Symp. Access Control Models Technol.*, Indianapolis, IN, USA, 2017.

[32] M. Jakobsson, E. Shi, P. Golle, and R. Chow, "Implicit authentication for mobile devices," in *Proc. 4th USENIX Conf. Hot Topics Secur.*, Montreal, QC, Canada, 2009.

[33] M. M. Koushki, B. Obada-Obieh, J. H. Huh, and K. Beznosov, "Is implicit authentication on smartphones really popular? On Android users' perception of 'smart lock for Android,'" in *Proc. 22nd Int. Conf. Hum.-Comput. Interact. Mobile Devices Services*, 2020, pp. 1–17.

[34] H. Khan, A. Atwater, and U. Hengartner, "A comparative evaluation of implicit authentication schemes," in *Proc. Int. Workshop Recent Adv. Intrusion Detection*. New York, NY, USA: Springer, 2014, pp. 255–275.

[35] Y. Xiao and M. Watson, "Guidance on conducting a systematic literature review," *J. Planning Educ. Res.*, vol. 39, no. 1, pp. 93–112, Mar. 2019.

[36] P. K. Mungai and R. Huang, "Using keystroke dynamics in a multi-level architecture to protect online examinations from impersonation," in *Proc. IEEE 2nd Int. Conf. Big Data Anal. (ICBDA)*, Mar. 2017, pp. 622–627.

[37] R. Bawarith, D. Abdullah, D. Anas, and S. Gamalel-Din, "E-exam cheating detection system," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 4, pp. 176–181, 2017.

[38] Y. Atoum, L. Chen, A. X. Liu, S. D. H. Hsu, and X. Liu, "Automated online exam proctoring," *IEEE Trans. Multimedia*, vol. 19, no. 7, pp. 1609–1624, Jul. 2017.

[39] Y. Khlifi and H. A. El-Sabagh, "A novel authentication scheme for E-assessments based on student behavior over E-learning platform," *Int. J. Emerg. Technol. Learn.*, vol. 12, no. 4, pp. 62–89, 2017.

[40] M. Durcheva and A. Rozeva, "Authentication with Tesla system instruments supporting eAssessment models in engineering courses," in *Proc. AIP Conf.*, 2019, Art. no. 040003.

[41] M. A. Haytom, C. Rosenberger, C. Charrier, C. Zhu, and C. Regnier, "Identity verification and fraud detection during online exams with a privacy compliant biometric system," in *Proc. ICETE*, 2020, pp. 451–458.

[42] A. Subash and I. Song, "Real-time behavioral biometric information security system for assessment fraud detection," in *Proc. IEEE Int. Conf. Comput.*, Nov. 2021, pp. 186–191.

[43] J. S. Ashwinkumar, H. S. Kumaran, U. Sivakarthikeyan, K. P. B. V. Rajesh, and R. Lavanya, "Deep learning based approach for facilitating online proctoring using transfer learning," in *Proc. 5th Int. Conf. Comput., Commun. Signal Process. (ICCCSP)*, May 2021, pp. 306–312.

[44] Z. Chen, H. Cai, L. Jiang, W. Zou, W. Zhu, and X. Fei, "Keystroke dynamics based user authentication and its application in online examination," in *Proc. IEEE 24th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2021, pp. 649–654.

[45] A. Zamfiroiu, D. Constantinescu, M. Zurini, and C. Toma, "Secure learning management system based on user behavior," *Appl. Sci.*, vol. 10, no. 21, p. 7730, 2020.

[46] Z. Zhang, M. S. Zhang, Y. Z. Chang, S. K. Esche, and C. Chassapis, "A virtual laboratory combined with biometric authentication and 3D reconstruction," in *Proc. ASME Int. Mech. Eng. Congr. Expo.*, 2016, Art. no. V005T06A049.

[47] P. Arias-Cabarcos, C. Krupitzer, and C. Becker, "A survey on adaptive authentication," *ACM Comput. Surveys*, vol. 52, no. 4, pp. 1–30, Jul. 2020.

[48] A. Amigud, J. Arnedo-Moreno, T. Daradoumis, and A.-E. Guerrero-Roldan, "An integrative review of security and integrity strategies in an academic environment: Current understanding and emerging perspectives," *Comput. Secur.*, vol. 76, pp. 50–70, Jul. 2018.

[49] X. Baró-Solé, A. E. Guerrero-Roldan, J. Prieto-Blázquez, A. Rozeva, O. Marinov, C. Kiennert, P.-O. Rocher, and J. Garcia-Alfaro, "Integration of an adaptive trust-based e-assessment system into virtual learning environments—The Tesla project experience," *Internet Technol. Lett.*, vol. 1, no. 4, p. e56, Jul. 2018.

[50] E. Al-Alkeem, S.-K. Kim, C. Y. Yeun, M. J. Zemerly, K. Poon, and P. D. Yoo, "An enhanced electrocardiogram biometric authentication system using machine learning," *IEEE Access*, vol. 7, pp. 123069–123075, 2019.

[51] G. Bradski, *OpenCV: Open Source Computer Vision Library*. 2015.

[52] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: Unified, real-time object detection," 2015, *arXiv:1506.02640*.

[53] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep face recognition," in *BMVA*, 2015, pp. 1–12.

[54] M.-C. Popescu, V. Balas, L. Perescu-Popescu, and N. Mastorakis, "Multilayer perceptron and neural networks," *WSEAS Trans. Circuits Syst.*, vol. 8, no. 7, pp. 579–588, 2009.

[55] C. H. Lin, J. C. Liu, and K. Y. Lee, "On neural networks for biometric authentication based on keystroke dynamics," *Sensors Mater.*, vol. 30, no. 3, pp. 385–396, 2018.

[56] T. R. Patil and S. S. Sherekar, "Performance analysis of Naive Bayes and J48 classification algorithm for data classification," *Int. J. Comput. Sci. Appl.*, vol. 6, no. 2, pp. 256–261, 2013.

[57] K. Sadeghi, A. Banerjee, J. Sohankar, and S. K. S. Gupta, "Performance and security strength trade-off in machine learning based biometric authentication systems," in *Proc. 16th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2017, pp. 1045–1048.

[58] K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," in *Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, Jun./Jul. 2009, pp. 125–134.

[59] Y. Sun, H. Ceker, and S. Upadhyaya, "Shared keystroke dataset for continuous authentication," in *Proc. IEEE Int. Workshop Inf. Forensics Security (WIFS)*, Dec. 2016, pp. 1–6.

[60] R. Giot, M. El-Abed, and C. Rosenberger, "Web-based benchmark for keystroke dynamics biometric systems: A statistical analysis," in *Proc. 8th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Jul. 2012, pp. 11–15.

[61] A. Okada, D. Whitelock, W. Holmes, and C. Edwards, "E-authentication for online assessment: A mixed-method study," *Brit. J. Educ. Technol.*, vol. 50, no. 2, pp. 861–875, Mar. 2019.

[62] S. G. Rabiha, A. Kurniawan, J. Moniaga, D. I. Wahyudi, and E. Wilson, "Face detection and recognition based e-learning for students authentication: Study literature review," in *Proc. Int. Conf. Inf. Manage. Technol.*, Sep. 2018, pp. 472–476.

[63] R. N. Pacheco, A. Dias, G. Santinha, M. Rodrigues, C. Rodrigues, A. Queirós, R. Bastardo, and J. Pav?o, "Systematic literature review of context-awareness applications supported by smart cities' infrastructures," *SN Appl. Sci.*, vol. 4, no. 4, p. 90, 2022.

[64] P. Wasnik, K. B. Raja, R. Raghavendra, and C. Busch, "Presentation attack detection in face biometric systems using raw sensor data from smartphones," in *Proc. 12th Int. Conf. Signal-Image Technol. Internet-Based Syst.*, Nov. 2016, pp. 104–111.

[65] C. B. Tan, M. H. A. Hijazi, N. Khamis, P. N. E. B. Nohuddin, Z. Zainol, F. Coenen, and A. Gani, "A survey on presentation attack detection for automatic speaker verification systems: State-of-the-art, taxonomy, issues and future direction," *Multimedia Tools Appl.*, vol. 80, nos. 21–23, pp. 32725–32762, Sep. 2021.

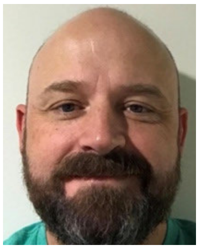
[66] Z. Rui and Z. Yan, "A survey on biometric authentication: Toward secure and privacy-preserving identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2018.

RISEUL RYU received the bachelor's degree in economics and the master's degree in information technology and systems from the University of Tasmania, Australia, in 2012 and 2019, respectively, where she is currently pursuing the Ph.D. degree.

She is a casual Academic Staff with the School of ICT, University of Tasmania. Her research interests include the development and application of cybersecurity software using machine learning, and blockchain technology with the Internet of Things.

SOONJA YEOM (Member, IEEE) received the master's degree in computing and the Ph.D. degree in haptic simulation in anatomy learning from the University of Tasmania, Australia.

She has been an Academic Staff Member and has held various administrative roles with the University of Tasmania, since 1994. Her research interests include natural language processing, big data technology in learning management systems, deep learning, affective computing, and educational technology. She is a member of the Working Group 3.3 (research into educational applications of information technologies) of IFIP/UNESCO.



DAVID HERBERT received the B.Sc. (Hons.) and Ph.D. degrees in artificial intelligence from the University of Tasmania, Hobart, in 1992 and 2020, respectively. From 1997 to 2016, he was a Senior Technical Officer and is currently a Lecturer with the School of Information and Communication Technology, University of Tasmania. His research interests include teaching and learning, knowledge base systems, natural language processing, educational technology, and cybersecurity.

JULIAN DERMOUDY is currently the Associate Head (Learning and Teaching) of the School of ICT and a Senior Lecturer with ICT. He has been a teacher for over 30 years and has received the Australian and University recognition for his teaching. He is the former Head of School, a Course Coordinator, and the Associate Dean. He is passionate about his teaching and his university. His research interests include learning and teaching, gamification and behavior change, and parallelism.