IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 27, 2021, accepted February 18, 2021, date of publication February 23, 2021, date of current version March 4, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3061589

Continuous Multimodal Biometric Authentication Schemes: A Systematic Review

RISEUL RYU[1], SOONJA YEOM[1], (Member, IEEE), SOO-HYUNG KIM[2], (Member, IEEE), AND DAVID HERBERT[1]

[1]Discipline of ICT, University of Tasmania, Hobart, TAS 7000, Australia
[2]Department of Artificial Intelligence Convergence, Chonnam National University, Gwangju 61861, South Korea

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

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2020R1A4A1019191).

ABSTRACT Building safeguards against illegitimate access and authentication is a cornerstone for securing systems. Existing user authentication schemes suffer from challenges in detecting impersonation attacks which leave systems vulnerable and susceptible to misuse. A range of research proposals have suggested continuous multimodal biometric authentication (CMBA) systems as a reliable solution. Though contemporary authentication systems have the potential to change their current authentication scheme, there is a lack of critical analysis of current progress in the field to foster and influence practical solutions. This paper provides a systematic survey of existing literature on CMBA systems, followed by analysis to identify and discuss current research and future trends. The study has found that many diverse biometric characteristics are used for multimodal biometric authentication systems. The majority of the studies in the literature reviewed apply supervised learning approaches as a classification technique, and score level fusion is predominantly used as a fusion model. The review has determined however that there is a lack of comparative analysis on CMBA design in terms of combinations of biometric types (behavioural only, physiological only, or both), machine learning algorithms (unsupervised learning and semi-supervised learning), and fusion models. Most of the studies evaluated a CMBA system's accuracy functionality, such as False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER). However, security, scalability and usability (user acceptance and satisfaction) are generally not addressed thoroughly even though these are key factors for system success in a real deployment. Furthermore, a CMBA system should be implemented and evaluated extensively on real data without restriction to prove that such systems are feasible.

INDEX TERMS Biometrics (access control), continuous authentication, machine learning algorithms, multimodal.

I. INTRODUCTION

User authentication is widely used as a means to protect any information technology (IT) system against unauthorized user activities [1]. Users are required to verify or authenticate their claimed identity, typically using credentials such as a username and password in order to then be granted specific privileges to access system resources. As IT is closely enmeshed in our daily lives, reliable and trustworthy authentication is extremely important as the primary step to ensure the information security within any IT system [2]. For more than 40 years there has been intense research in authentication methods - this acknowledges the crucial importance of the authentication process to build trustworthy and secure environments that defend against impersonation of a user's identity, yet at the same time also attempting to alleviate or simplify the complexities of the authentication process itself [3].

Authentication and verification of a user can be achieved by utilizing one or more of three fundamental, broad approaches: knowledge-based (something a user knows), possession-based (something a user has), and biometric-based (something a user is). The first two approaches have been widely adopted in most IT systems; however, they face many well-known challenges. The latter approach, biometric-based authentication, which uses physiological and behavioural characteristics of a user, has gained popularity as a reliable solution [1]. Even though this

The associate editor coordinating the review of this manuscript and approving it for publication was Zahid Akhtar.

approach provides remedial benefits to counter deficiencies in the former approaches, most solutions only use a single biometric cue that is merely applied at the point-of-entry (known as static authentication). This weakness can be argued as being insufficient to provide a verifiably secure system [1], [2], [4]. Using a single biometric factor potentially lowers the authentication system's accuracy rate due to poor data quality, the overlap between identities and limited resources to uniquely identify a person [4]. Furthermore, a single biometric factor used with static authentication means the underlying system could be vulnerable to being misused post-authentication due to the apparent permanency of verification of the user identity for the session [1], [5].

Continuous multimodal biometric authentication has emerged to improve recognition accuracy and mitigate the challenges in the static one-time authentication process [2], [6], [7]. However, usability and scalability issues have arisen as CMBA requires re-verification of the user's claimed identity to the system repeatedly and it collects the user's biometric cues to improve its accuracy [1], [4]. Although there are in-depth studies of surveys that analyse biometrics [8] and the fusion of multimodal biometrics for implicit authentication [7], no work has yet provided a comprehensive systematic review of the combined use of different biometrics for continuous authentication. Existing surveys are limited by the fact that they adopt a more general focus on continuous authentication systems [2] or the classification of biometric authentication [4], [9]. To fill this gap, we conduct a systematic literature review on continuous multimodal biometric authentication.

The paper aims to formalize the findings of state-of-art continuous multimodal biometric authentication systems through their design, implementation, and evaluation methods. We survey how the literature to date have fused multimodal biometric data to authenticate users continuously. The paper aims to identify how multimodal biometrics are proposed and evaluated for continuous user authentication, what is missing in the studies, and to elicit a roadmap for the research body to help move forward. The main contributions are: 1) Survey, systematization and analysis of continuous multimodal biometric authentication approaches in the academic literature to date, 2) Providing insights on continuous multimodal biometric authentication systems from multiple perspectives, and 3) Identification and discussion of current research challenges and future directions.

The paper is presented as follows: Section 2 introduces the related surveys, then we present the concept of biometric authentication systems in section 3. The systematic review methodology is described in section 4, following the motivation of the study and the research question. The results are analysed and interpreted in section 5. Section 6 offers a consolidated overview of the work and it provides a critical discussion eliciting future work before conclusions are drawn in section 7.

II. RELATED SURVEYS

In 2015, Gad, *et al.* [10] reviewed multimodal biometric systems by identifying the integration of the biometric factor data, quality performance, and fusion levels in multimodal biometrics. The survey investigated the generic overview of a multimodal biometric system, identifying its opportunities and challenges for security purposes. Even though these reviews are considered significant, the literature coverage is rather limited. Al Abdulwahid, *et al.* [1] put a specific focus on CMBA feasibility in practice by reviewing the critical achievements in adopting a CMBA system to authenticate users continuously. However, the survey does not discuss how they combine different biometric factors to build a continuous and transparent CMBA system as they have focused on its performance evaluation. One identified study has surveyed the biometric fusion method [4], but the study does not consider whether the authentication is static or continuous. Another recent study [11] systematically reviews biometric authentication systems, but the review is conducted on both unimodal and multimodal biometric systems. While these works provide detailed analysis and valuable insights on biometric authentication systems, they are not concerned with the authentication modes (static or continuous).

Several identified studies reviewed continuous authentication systems, and they are focused on either general continuous authentication systems [2] or biometric authentication systems [5], [8], [12]. The majority of the reviews on continuous biometric authentication systems narrow their scope into a specific authentication domain such as mobile [8], [12] or behavioural biometrics only [5], that could cause different design or implication challenges. There is a need to systematically review CMBA systems by not limiting the authentication domain or the types of biometrics used. This helps in the decision process for choosing adequate authentication schemes for different user contexts along with the most used criteria for the comparison and selection. It could be useful for researchers as well as industry experts to determine how to select the most appropriate continuous authentication scheme for their application and purpose. Therefore, our paper systematically covers research work on continuous authentication using multimodal biometrics to analyse how they have applied biometric characteristics in continuous authentication systems and their performance evaluation. We further discuss specific challenges for CMBA systems and establish a research roadmap intended to foster advancement on the topic and influence real-world implementations.

III. MULTIMODAL BIOMETRIC SYSTEMS

Biometric authentication systems have gained popularity to verify user identities over many decades due to their reliability and adaptability. Existing biometric authentication systems generally consist of various processes depending on the biometric information, including physiological and behavioural features. The physiological feature is based on an individual's unique physical traits (e.g., fingerprints and facial features), and behavioural features refers to

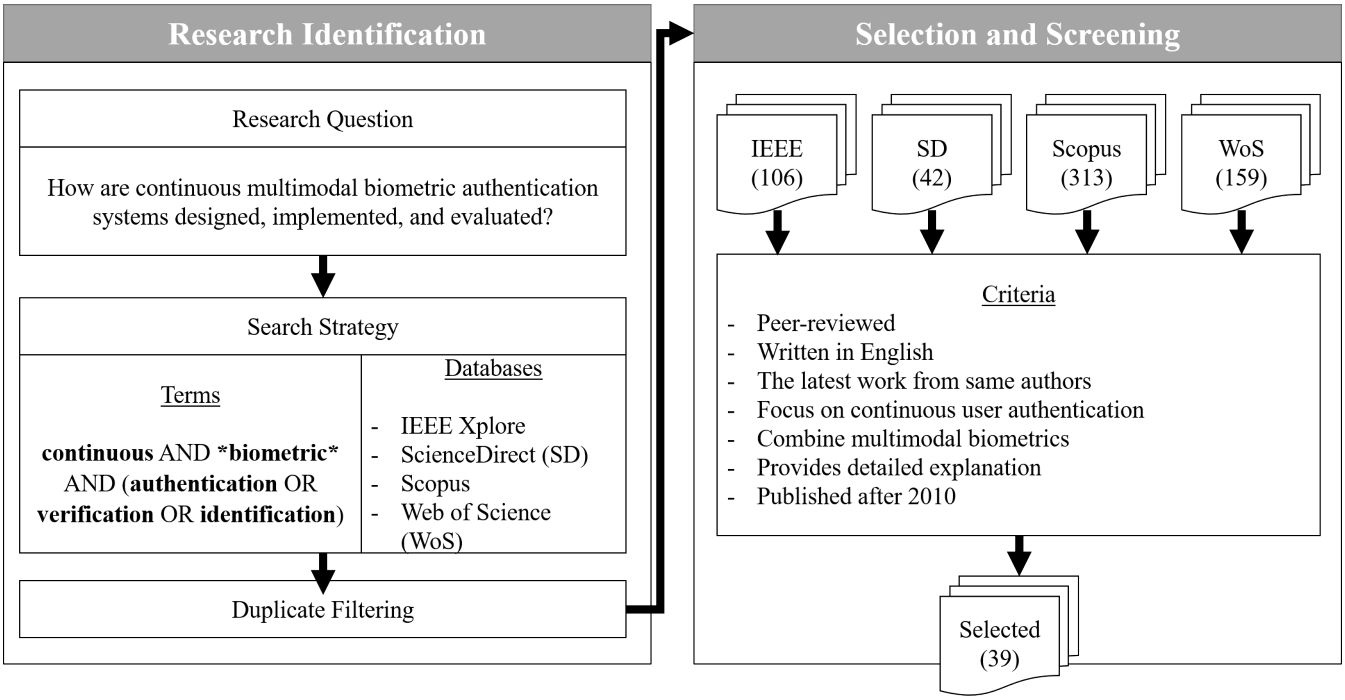
Research Identification
Research Question
How are continuous multimodal biometric authentication systems designed, implemented, and evaluated?
Search Strategy
Terms
continuous AND *biometric* AND (authentication OR verification OR identification)
Databases
- IEEE Xplore
- ScienceDirect (SD)
- Scopus
- Web of Science (WoS)
Duplicate Filtering
Selection and Screening
IEEE (106)
SD (42)
Scopus (313)
WoS (159)
Criteria
- Peer-reviewed
- Written in English
- The latest work from same authors
- Focus on continuous user authentication
- Combine multimodal biometrics
- Provides detailed explanation
- Published after 2010
Selected (39)

FIGURE 1. Summary of the procedure for identifying and selecting the relevant literature on continuous multimodal biometric authentication systems, following PRISMA Guidelines [13] and the Joanna Briggs institute Reviewer's manual [14].

an individual's behaviour and personality pattern (e.g., gait (walking) analysis, keystroke dynamics) [10]. The authentication process is initiated with the sampling of specific biometric traits, followed by pre-processing, finding the area of interest, extracting pre-determined features using feature extraction algorithms, and implementing classification algorithms for the decision-making process [11]. Novel feature extraction and classifiers can also be developed and used.

Depending on the number of the modalities used, a biometric system can be classified into two types: unimodal or multimodal. Unimodal biometric systems rely on a single modality for authentication and they are easier to develop as they are based on a single identifier. However, a unimodal system faces challenges such as noisy data, poor recognition performance, less accurate results, and spoofing attacks, as the authentication metric itself can be a single point of failure [1], [10], [11]. A multimodal biometric system in contrast, employs multiple or complementary traits (e.g., face and voice features), does not rely on a single feature and is thus much more robust and difficult to defeat. It is more secure from spoofing attacks [11], provides high recognition rates, is less sensitive to the impact of environmental factors, and has increased robustness and reliability [10]. As multimodal biometrics uses more than two biometric cues for authentication, when fusing the information from different modalities it must consider answering the following questions: 1) *what* to combine, 2) *when* to fuse and 3) *how* to fuse to develop a multimodal biometric authentication system [4]. *What to fuse* involves selecting different biometric traits to be combined, such as face and voice, or fingerprint and keystroke dynamics. *When to fuse* determines the level of fusion in which the individual biometric factors can be fused in the pipeline stages of the biometric authentication system. *How to fuse* refers to the method that is used to consolidate the information. This paper therefore presents a comprehensive analysis of information fusion techniques combined with the multimodal biometric authentication system design, including classifier algorithm chosen, for each modality.

IV. METHODOLOGY

The study aims to investigate the design, implementation, and evaluation method of continuous multimodal biometric authentication systems. The objectives of the study are to identify CMBA schemes proposed in literature, to appraise the evaluation methods used for the suggested CMBA schemes – as well as the datasets they have employed, and to suggest future directions to empower knowledge in the area. Based on these objectives, the study focuses on analysing how the literature covers continuous multimodal biometric authentication systems, what can be learned, and what is missing in order to advance research in the field. The following research question has been driven with five sub-components (Table 1) to address the problem statement: *How are continuous multimodal biometric authentication systems designed, implemented, and evaluated*?

We conduct a systematic review based on PRISMA guidelines [13] and the Joanna Briggs institute reviewer's manual [14] to ensure a comprehensive and unbiased systematic review (Fig. 1). We identify relevant studies on continuous multimodal biometric authentication systems as described in Fig. 1. Based on the research question, a search protocol

TABLE 1. Five sub-components and corresponding motivation to answer the main research question.

	Question	Motivation
SRQ1	What biometric cues are used?	To identify the various biometric features that are used by authentication methods.
SRQ2	What classification algorithms are used?	To identify the dominantly used classifiers and how they perform.
SRQ3	How are different modalities fused?	To identify how the source of information has been fused in the authentication process.
SRQ4	What are measures used to evaluate the performance of the authentication system?	To identify the various metrics used for performance evaluation and to seek to identify newer performance evaluation methods.
SRQ5	What is the dataset used to evaluate the performance (how many users/records are used to test the proposed authentication technique)?	To identify experiments with re-usable or reachable datasets. It will also provide information about the performance of a particular dataset.

is developed to guide the process to reduce the researcher's biases in study selection. We use search keywords "continuous biometric authentication" and the semantically similar terms "verification" and "identification". We also use a wildcard (∗) to allow for variations of the terms so that the use of wildcards assists overcoming the differences in grammar and formatting in articles. For example, the term "*biometric*" could return biometric, -biometric, biometrics. We use four databases in the study, Institute of Electrical and Electronics Engineers (IEEE) Xplore [15], Science Direct [16], Scopus [17] and Web of Science [18] to cover a wide range of information technology literature. We compile works containing a set of 620 articles spanning from 2010 to June 2020 after removing duplicates based on the search term. The exclusion criteria are attempted to remove irrelevant data. Papers are excluded if:

1) The publication format was not a peer-reviewed academic journal or conference paper.
2) The publication language was not in English
3) Another paper by the same authors superseded the work, in which case the latest work is considered.
4) The proposed authentication process is static, not continuous.
5) The paper does not combine multimodal biometrics for authentication purposes.
6) The approach is described at a high level, and not enough detail is provided to address the research question.
7) Paper was published before 2010.

Once a stepwise process of the screening article title, keywords, abstracts, and full papers against exclusion criteria is undertaken, one hundred and twenty-four (124) articles are screened at the final stage (Table 2). Thirty-nine (39) articles are included in the analysis of continuous multimodal biometric authentication systems.

TABLE 2. The summary of the exclusion reasons for screened full-text articles.

Reason for exclusion	Number of articles
Preliminary studies (no implementation conducted)	9
Not continuous user authentication	20
Out of scope (i.e., data storage for authentication is focused, use one biometric cue, authentication system focused not limiting the use of biometric information for authentication, not a recent work)	40
Other reports (i.e., review article, editorials, lecture note, proposals)	16
Total	85

V. RESULTS AND ANALYSIS

The focus in this section is on thirty-nine (39) selected publications (see Appendix). Depending on the scope of the focused platform or adaptation, the final corpus is sub-categorized in four clusters: 1) computer, 2) mobile devices, 3) wearable devices/internet of things or 4) other types (Table 3).

A. BIOMETRIC AUTHENTICATORS

Biometric authenticators are the managed biometric resources of the authentication system, which is the feature that needs to be adapted. Biometrics is broadly classified as *something you are*, the means of identifying humans using their traits or characteristics [2].

Table 3 shows the biometric features covered in continuous authentication literature, divided according to three-dimensional categorization [8], [12], [57]: behavioural, physical, and soft. Behavioural biometrics are the attributes describing the behaviour or personality of an individual, for example, keystroke dynamics, touch behaviour, gait, speech, behaviour profiling, and more [8]. Physiological characteristics are based on parts of a human's body, which include the face, iris, ear, fingerprint, palm print, and vein [2]. Soft biometrics have ancillary characteristics based on the description of human physical features such as gender, skin colour, scars, ethnicity, and height [57].

Physiological traits are widely used in an authentication system because of their unique characteristics such as their near-permanence, ease of collection, and uniqueness and they are relatively inexpensive techniques for verifying an identification [11]. Additionally, physical features are more unvarying over time and under different conditions when compared to behavioural features due to the variability of a user's behaviour – behaviours can commonly change depending on mood, illness, stress, previous events, environment, etcetera.

Even though physiological features are widely used in an authentication system, it is observed that 46% of papers only combine behavioural traits. In comparison, 28% of papers choose to combine physiological traits due to their high uniqueness, distinction [28], [52], non-invasiveness [51], and stability [34] (Fig 2 and Table 4). Behavioural biometrics are preferred as they can be collected in a non-intrusive way and continuously [37], and they generally do not require

TABLE 3. Overview of biometric authenticators used in continuous multimodal biometric authentication systems.

	Work	Behavioural												Physiological								Soft
Category		Keystroke/typing	Mouse	Gesture	Touch	Phone Movement	Speaking	Linguistic style	Haptic	Gait	Wrist	Behaviour profile	Voice	Face	Ear	Iris	Fingerprint	Palm	Electroencephalography (EEG)	Electrocardiogram (ECG)	Blood Volume Pulse (BVP)	Skin Colour
Computer (PC, Laptop)	[19]	x	x																			
	[20]	x												x								
	[21]	x	x					x														
	[22]																			x	x	
	[23]	x	x																			
	[24]	x	x																			
	[25]													x	x	x						
	[26]	x	x																			
	[27]	x	x						x	x												
	[28]													x		x	x	x				
	[29]	x												x			x					
	[30]	x												x								
	[31]	x	x																			
	[32]	x												x								
	[33]																x			x		
	[34]													x		x						
Mobile devices	[35]	x		x		x																
	[36]	x						x				x										
	[37]	x						x				x										
	[38]									x		x										
	[39]				x									x								
	[40]			x	x																	
	[41]					x								x								
	[42]	x		x																		
	[43]				x	x																
	[44]	x					x															
	[45]	x			x																	
	[46]									x							x					
Others (i.e., network)	[47]												x				x					
	[48]													x			x					
	[49]															x	x					
	[50]															x	x					x
	[7]	x												x								
	[51]													x					x			
	[52]												x	x								
Wearable devices/IoT	[53]													x		x						
	[54]	x									x											
	[55]		x								x											
	[56]				x								x									

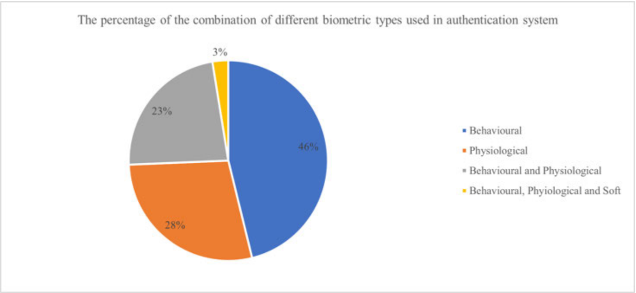

FIGURE 2. The ratio of the combined different biometric types in the authentication system.

TABLE 4. Overview of the biometrics combination used in multimodal.

Biometric traits	Number of papers
Behavioural	18
Physiological	11
Behavioural and Physiological	9
Behavioural, Physiological and Soft	1

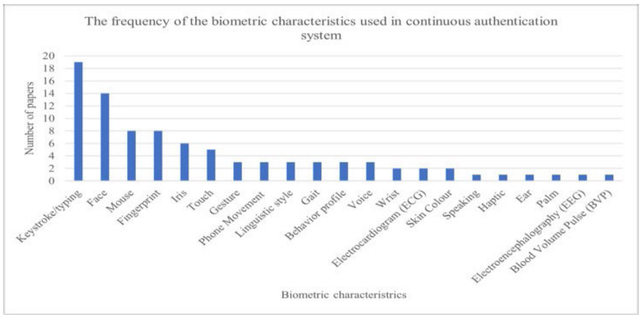

FIGURE 3. The frequency of the biometric characteristics used in the continuous authentication system.

any additional hardware for data captures such as a camera or fingerprint scanner [24], [37]; therefore, they may be more cost-effective and user-friendly methods [23]. It is also expected that using behavioural biometrics is less computationally complex compared to other physiological biometric cues (i.e. fingerprint or face) because of the limited amount of information collected [24].

Overall, 23% of papers mix behavioural and physiological cues for an authentication system. Combining different types of biometric data could improve performance and measurability by complementing each other [20], [29], [30], [32], [46], [56]. Keystroke dynamics and face recognition are a dominant combination of the biometric characteristics among the reviewed papers as both do not require any additional devices or interaction with a separate sensor directly (as most systems already have a keyboard and web camera), and the data collection does not interrupt genuine user activity [20]. Keystroke dynamics can complement face recognition when authentication through facial images alone shows lower performance due to sensitivity to light levels and face distance from the camera. On the other hand, a high measurability rate of facial images can cover temporal gaps in keystroke capture when keystroke dynamics acquisitions are missing [29], [30]. Schiavone, *et al.* [29] use a particular kind of mouse that contains a fingerprint scanner to avoid any additional device and interruption of user activity when measuring fingerprints.

This study has found that researchers are more interested in multimodal behavioural biometric authentication systems because they enable continuous and non-intrusive authentication schemes without the need of additional devices compared to physiological characteristic-only measurement schemes.

Regardless of the authentication system's targeted platform and the combination of several types of biometric features, keystroke dynamics and face recognition are the dominant characteristics used in authentication systems (Fig 3 and Table 3). Keystroke dynamics is a behavioural biometric that intends to gather an individual's typing style on a keyboard as a regular part of the device [7], [37]. Therefore, it has a low implementation cost, as no specific additional hardware is required [54]. It is also non-intrusive, transparent [44] and a user's typing style is hard to mimic [7]. As it provides sufficient discrimination information to allow identity authentication, despite the fact that keystroke dynamics has been shown to not necessarily be unique for each person [37], keystroke dynamics is widely adopted in continuous authentication systems when combined with other traits [7], [37].

The human face is another dominant biometric trait used in various applications due to its contactless process and low implementation cost compared to other physiological biometric traits such as iris or fingerprint [7], [11]. However, facial recognition still suffers some limitations as face recognition performance can be less effective due to variations in facial expressions, angles, and illumination [11], [34], [58]. To overcome these limitations, other physiological biometrics such as iris are becoming increasingly popular in continuous authentication systems [11].

Touch gestures, fingerprints, and voice recognition have been found to be gaining more attention which coincides with increasing usage of smart device mobile applications [12], [47]. Touch and typing gestures becomes the dominant authentication techniques in mobile platform as touch-enabled phones and tablets (e.g., iPhones, iPads, Samsung Galaxy) have increasingly widespread ubiquity. Touch gestures can be used as an effective biometric factor to continuously authenticate users without interrupting a user's activity in the background [12], [56]. Fingerprint recognition has been implemented on most touch-enabled devices as a static entry-point authentication method [8]. This is most evident in the public domain as the majority of smartphones have a fingerprint sensor for this authentication purpose.

Additionally, users can use fingerprint authentication combined with their touch gestures [8]. Voice recognition is also widely adopted in a mobile platform to assist users (e.g., Siri) [8] and for user interactions on wearable devices [56]. As voice features can be extracted through voice commands on the mobile phone or wearable devices, it does not require special additional devices in the acquisition process. Therefore, voice recognition can be easily applied and accepted for remote authentication [52]. However, the reliability and accuracy rate of voice recognition is comparatively low as the performance depends on several environmental conditions, so adding other biometric traits such as touch gestures or fingerprints may compensate for the current weakness that voice recognition has [56].

The papers that have been reviewed clearly explain the benefits of using multimodal biometrics by comparing their examination results with unimodal results [20], [29], [30], [32], [46], [56]. However, there is no comparative analysis of the accuracy between behavioural- or physiological-only systems and composite systems of behavioural, physiological and soft biometrics. The performance of the different combinations of biometric types could be compared through benchmarks; however, non-conformity in experimental setup such as data collection, hardware systems and the authentication architectures make accurate comparisons difficult.

It is observed that the majority of the literature reviewed combines two different modalities; seven papers combine three different biometric cues and two papers suggests the combination of four different modalities. However, the research contains no further discussion or insight as to how many different modalities (for example two or more than two modalities) could optimise the accuracy of the system based on localised domain constraints.

B. CLASSIFICATION ALGORITHMS

Several algorithms and techniques are used in the various authentication systems to classify the features of the biometric data. Machine learning approaches are widely adopted in authentication systems as they promise more accuracy and efficient security [12], [59]. Among the different types of machine learning approaches (supervised, unsupervised, semi-supervised, and reinforcement learning), it is observed that the supervised machine learning techniques (k-Nearest Neighbours (k-NN), Naïve Bayes (NB), Random Forest, and more) are dominant (Fig. 4).

While most of the biometric traits are used in supervised learning for classification, facial recognition prefers Principal Component Analysis (PCA), which is considered an unsupervised learning technique (Fig. 5). This is because unsupervised learning does not make any assumptions about pose or expressions to recognize faces in unconstraint environments [60].

The difference between supervised and unsupervised learning is that supervised learning requires a labelled dataset which provides known classifications to evaluate its accuracy on the training dataset whereas unsupervised learning does not need prior knowledge for the corresponding inputs [59]. In general, supervised learning techniques tend to be more accurate than unsupervised learning; however, they require large training corpora that could require retraining if applied to other domains, and they also suffer from over-training issues [61]. Supervised learning algorithm's performance accuracy is directly related to the size of the training set – if adequate, labelled data is not available, performance suffers. [31]. The selection of supervised and unsupervised machine learning techniques are in essence a trade-off between accuracy and generality [61]. Therefore, the choice of supervised or unsupervised machine learning techniques depends on the volume of training data at hand and the focus of the authentication system [59]. As the two approaches have yet to be compared in the same multimodal biometric authentication system, it is still an open question of which method is better for continuous multimodal biometric authentication.

A semi-supervised learning algorithm is a mix of supervised and unsupervised learning. It uses a massive amount of unlabelled data with a small amount of labelled data to overcome the problem in both supervised techniques and unsupervised techniques [62]. Semi-supervised learning techniques have outperformed both supervised and unsupervised techniques in face identification authentication applications [62];

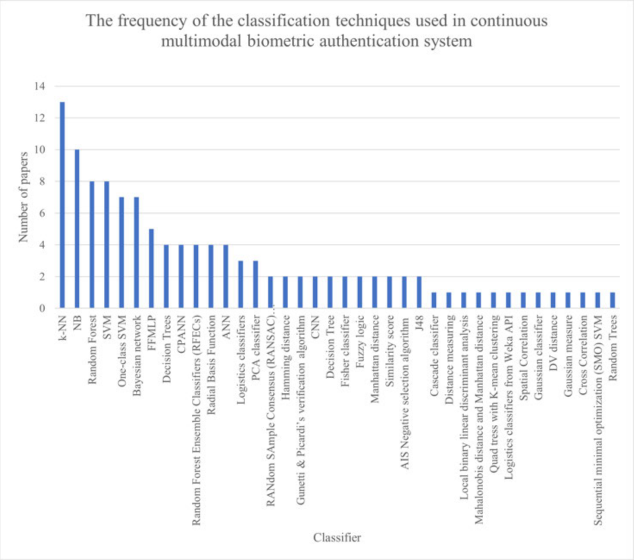

FIGURE 4. The frequency of the classification techniques used in the continuous multimodal biometric authentication system.

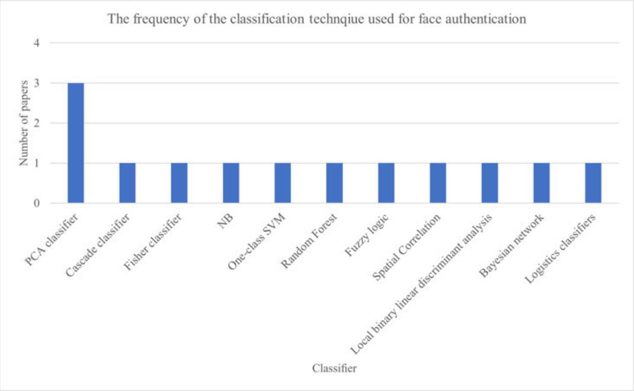

FIGURE 5. The classifier frequency used in face authentication.

however, this technique has not been explored and examined thoroughly in multimodal biometric authentication systems.

Reinforcement learning does not require accurate inputs and outputs but learns to make a sequence of decisions in an uncertain or complex environment based on each action's reward. As it requires the simulation environment to learn (which is highly dependent on the task to be performed), it may not be suitable when there are limitations in available resources and time [59].

Some researchers use more than one classifier for their experiments to identify the best classifier amongst the group of classifiers they selected [31], [45], [52]. El-Bendary, *et al.* [52] and Putri, *et al.* [45] choose more than one classifier to find the best classifiers among them. It was found that the Gaussian Mixture Model (GMM) is the best classifier for voice and face authentication rather than ANN and SVM [52]. It is also observed that the best classifier can be different depending on the extracted features; for example, the most accurate classifier is BayesNet for keystroke dynamics features, and Random Forest for tapping, swiping and pinching features [45].

Aljohani, *et al.* [31] compare different classifiers to the AIS Negative Selection (NS) algorithm, which is introduced in their paper for the keystroke dynamics and mouse movement authentication classifier. The research shows the profound effectiveness of NS algorithm over SVM and Decision Trees. As shown in other studies [40], more exploration of NS algorithms with other biometric features could give more concrete evidence for it to be used as an efficient classifier.

C. FUSION LEVELS

The primary condition for a CMBA system's success is determined based on 1) the type of information used in the system and 2) the methodology used for fusion [54].

Score level fusion compares a feature's value, and then similarity scores generated from each modality are combined to form a single fused score. It is commonly used in CMBA systems as the matching score can be easily obtained and it provides sufficient discrimination information to distinguish a genuine user from impostors [40], [47]. Within the score level fusion mechanism, each modality operates independently; hence additional biometric modalities can be incorporated in the authentication system by simply adding a modality [51]. The most widely used technique in score level fusion is weighted sum rule which gives different weights on each modality scores depending on its success and accuracy of authentication when the resulting scores from each modality are combined [20], [23], [30]. Quality-based score level fusion is suggested, which uses quality information of the original features to then determine each modality's weight to compute a single score in order to improve authentication performance [41]. Experiments reveal that including quality information results in better performance in comparison to fusion scores without quality information.

The second dominant fusion scheme used in CMBA systems is feature level fusion which combines different features extracted from raw biometric data into a single template [7], [47]. This process can eliminate noise in the raw biometric data, thus potentially improving authentication recognition [47]. Feature level fusion allows the de-identification of images and feature sets by generating a new biometric image or feature set for authentication which can also obscure the identity of the original biometric image [49], [53]. However, due to the high-dimensionality of data, feature level fusion generates a higher-computational load [51]. To ameliorate this effect, the Random Forest Ensemble Classifier (RFEC) is used to deal with high-dimensional features and handle high variance data [55]. Furthermore, high-dimensionality is also addressed by the 2-Dimensional Winner-Takes-All Hashing (2DWTA) [47].

Decision level fusion is similar to score level fusion, but it converts the score into a match or non-match result before the fusion [7]. Recognition results are classified into either *accept* or *reject* which is more convenient and relatively easier to fuse without recreating the detection algorithm to determine the fusion level's authentication results [21].

Rank level fusion treats the system's output as a ranking of the enrolled user identities [63]. The set of possible matching identities is sorted in descending order of confidence to derive a consensus rank for each identity [46]. Ranks are then used in the decision-making process to identify the best match. The ranking output generated from multiple biometric systems is comparable and thus normalization of each classification result in score level fusion is not required [63]. This makes rank level fusion simpler than score level fusion and it consumes less processing time than feature level fusion [46].

Several of the surveyed papers attempt to find the optimal fusion level by comparing their performance in order to maximize the authentication system's performance [33], [35], [52]. Comparisons between score level and feature level for swipe gestures and phone movement patterns shows that feature level fusion outperforms score level (93.33% and 89.31% respectively) [35]. However, score level (EER = 0.69%) indicated better performance than feature level fusion (EER = 2.81%) with voice and face feature datasets [52]. Two major differences between two studies [35], [52] are the biometric traits they have combined, and the classification algorithm used. This leads to an interpretation that the accuracy and performance of the fusion level could significantly vary depending on the biometric traits and classification algorithm considered by the system.

Two approaches compared using fingerprints and ECG with the Convolutional Neural Network (CNN) model [33]. In this referenced work, decision level fusion follows a sequential pattern, beginning with ECG authentication, proceeded by fingerprint authentication. For feature level fusion, a parallel system extracts a feature vector from the ECG image and fingerprint image, and then it combines both vectors to create a new feature vector to represent the presented identity. The results reveal that the sequential system based on decision level performs better than the parallel system based on feature level in terms of the recognition accuracy rate, but at the cost of an increased computation time. As there is no further discussion, investigating the reasons behind the finding could give more insights into whether a system structure such as parallel or sequential recognition could impact the accuracy of authentication performance.

Score level fusion is the most common (and preferred) fusion technique as implementations are readily available and it provides good discriminatory performance to distinguish between a genuine user and an imposter [9], [51]. However, there is a lack of discussion as to whether score level fusion provides the highest performance among different fusion levels (sample, feature, score and rank). Depending on the platform, the target system – such as computer, mobile or wearable, and combined biometric traits, different fusion levels could provide different performance results [35], [52]. Therefore, a major recommendation for future studies is to conduct performance comparisons among different fusion levels to gain insight into how to fuse biometric data to optimize the authentication system's accuracy.

D. PERFORMANCE EVALUATION

Various metrics have been used to evaluate the proposed authentication systems (Table 5). The evaluation criteria most used is the accuracy of the authentication system. Among various performance indicators, false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (ERR) are predominant. FAR indicates whether the model is good at blocking illegal access [12] by calculating the ratio of the false acceptance rate to the total number of acceptances [28], [41]. FRR calculates the ratio of the valid users who should be authentic to the system but are still rejected [7], [54]. EER is the error rate at which both FAR and FRR are equal [56]. EER is also widely used together with FAR and FRR to measure biometric systems [7].

False Match Rate (FMR) and False Non-Match Rate (FNMR) are another set of performance measures widely used to evaluate biometric systems [23]. FMR measures the probability of incorrectly authenticating a non-legitimate user as a legitimate user, while FNMR calculates the probability of the system wrongly rejecting legitimate users [50]. However, only Sahayini and Manikandan [50] solely use FMR and FNMR to evaluate their proposed CMBA system. Average Number of Genuine Action (ANGA) and the Average Number of Imposter Actions (ANIA) are introduced as new performance measures, the authors claiming that FMR and FNMR are no longer valid for a continuous biometric authentication system [23]. To continuously authenticate users, each separate action performed by a user should be considered in the imposter detection process in as few actions as possible [20], [23], [24].

As there is no unified standard for performance metrics, it is difficult to determine which performance indicator provides reliable accuracy results for evaluation of CMBA systems' performance. Therefore, discussion of different performance indicators used in the literature is warranted as a starting point to construct the unified accuracy performance metrics for a continuous biometric authentication system.

Scalability is the system's ability to ensure that there is no impact on its performance regardless of the system size [64]. A system's scalability is critical to its long-term success [65] since the number of users may vary over time [64]. Fridman *et al.* [21] measured the scalability of a CMBA system by comparing the first authentication time taken with system loads of between ten users and sixty-seven users. The authentication performance time increased with sixty-seven users compared to ten users, but it was not significant; hence, the system measured may be scalable in a closed world environment [21]. A caveat though is the performance was compared only for the *first* authentication time; it is unclear and unlikely as to whether scalability is guaranteed for continuous authentication where repeated measurements are required. Different indicators (packet delivery ratio, throughput, end-to-end delay, overhead cost, communication latency) are examined by comparing a new proposed authentication method and existing, classical methods [53]. Increasing the number of sensors from 20 to 120 shows there is a reduction in communication overheads, end-to-end delay, and delivery ratio for the proposed method [53]. However, the evaluation is focused on the system's efficiency, not scalability, so it could not conclude that the proposed method is scalable. A continuous authentication system should be flexible and scalable enough to accommodate new user addition and deletion for authentication [64]. As there is a dynamic change in the number of registered users over time, and such systems requires re-verification of active users repeatedly, the defined user base and active user load should not affect system authentication performance [1], [4]. Despite its importance, the feasibility of CMBA scalability has not been addressed in real-world deployments. Therefore, studies exploring scalability are needed to fill the gap.

Survey works [21], [39], [44], [47], [53] consider potential security threats. Possessing a multimodal biometric authentication system would harden the host system against authentication spoofing; if one biometric modality is compromised, additional biometric modalities will increase the authentication confidence [21], [39]. A trust model, which calculates the confidence level, whether a user is genuine or not, can protect the system when an attacker accesses the device [44]. The device confidence however is reduced and may still meet predefined confidence thresholds when the attacker can generate a biometric sample continuously, especially if they only have to satisfy one biometric modality. There is also a chance that the communication between two authentication parties is conducted through an unsafe channel [53]. Applying cryptographic protocols between system communication channels could help secure the system against Denial-Of-Service (DoS) attacks, node compromise attacks, and repudiation attacks [53]. There is also a possibility that devices can be stolen, lost, or shared among a group of individuals. Therefore, it is also essential to measure whether the system can secure devices when they are lost, stolen, and shared [38].

TABLE 5. The performance method used for evaluating each of the proposed authentication systems.

Category		Performance indicators	No. papers
Functionality		False Acceptance Rate (FAR), False Positive Rate	18
		False Rejection Rate (FRR), False Negative Rate	15
		Equal Error Rate (EER)	13
		Receiver Operating Characteristics (ROC)	9
		Accuracy	5
		False Match Rate (FMR)	3
		Average Number of Genuine Action (ANGA)	3
		Average Number of Imposter Actions (ANIA)	3
		False Non-Match Rate (FNMR)	2
		Genuine Acceptance Rate (GAR)	2
		Impostor Detection Rate (IDR)	2
		Success authentication	2
		Average Number of False Rejections (ANFR)	1
		True Acceptance Rate (TAR)	1
		Genuine Match Rate (GMR)	1
		False Alarm Rate	1
		True Positive Rate	1
		Cumulative Match Curve (CMC)	1
		Error Rate	1
		Half Total Error Rate (HTER)	1
		Error of Identification	1
		Area Under The Curve (AUC)	1
		Mean Detection Rate	1
Security		Stolen Attack	2
		Attack scenario	2
		Shared Attack	1
		Attack-via Multiplicity (ARM)	1
		Node compromise attack	1
		Non-invertibility analysis	1
		Spoofing	1
		Node Capture Attack	1
		Replay attack	1
		DoS attack	1
Usability	Operation time	Latency	2
		Verification Time	1
		Time to First Decision	1
		Mean Time To Impostor Rejection (MTIR)	1
		Time to extract feature	1
		Mean Authentication Time (MAT)	1
		Runtime	1
		Decision Delay	1
	Operation cost	Bandwidth	1
		Battery Usage	1
		Communication overhead	1
		Computation cost	1
		CPU usage	1
		Memory Usage	1
		Optimal Thresholds	1
		Packet Delivery Ratio (PDR)	1
		Storage Space	1
		Throughput (TP)	1
	Satisfaction/ Acceptance	User evaluation	2
	Stability	Availability to complete the task	1
		Percent Residual Difference (PRD) metric	1

Multimodal biometric authentication systems can secure the owner's sensitive resources against an imposter, whether they are an adversary, family member or co-worker [38]. The reliability of a feature template is worthy of further investigation because user authentication is based on the template [47]. However, a key challenge that remains unsolved that is a well-known public concern is the privacy of biometric data, which can reveal sensitive information about the user, specifically if this data is not locally stored or the computations are outsourced to a third party [3].

Usability for an authentication system is defined as the degree to which legitimate users can operate or perform particular tasks with an acceptable level of satisfaction, effectively and efficiency [66]. Therefore, usability can be measured by testing one or more constituent factors, including effectiveness, efficiency, and user satisfaction [32].

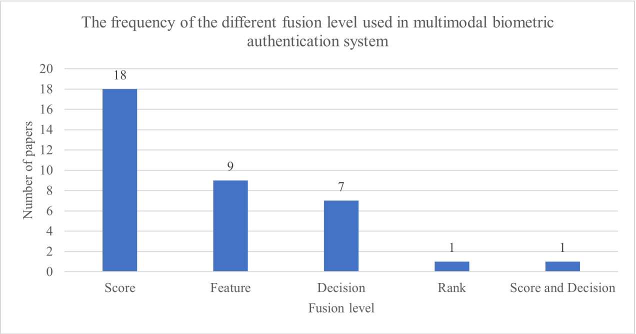

FIGURE 6. The frequency of the fusion level used in the multimodal biometric authentication system.

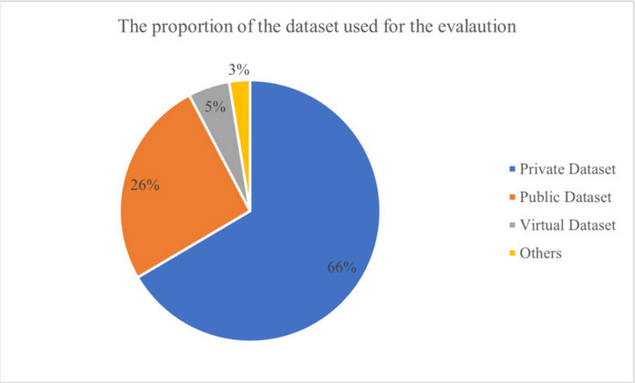

FIGURE 7. The type of the dataset used in the paper (public dataset, private dataset, virtual dataset and other).

Effectiveness is defined as the user's ability to successfully achieve operational goals. Efficiency is described as when a user can perform a particular task within an acceptable time frame successfully. Satisfaction simply measures a user's overall perception and acceptance of the authentication processes of the operating system [66]. In terms of efficiency of the authentication system, various time metrics are measured, including the detection latency of imposters (i.e., running time for decision making) [29], [36], [38], [39], communications [29], [38], [53], and computational latencies [38]. Operating costs are also measured, such as CPU usage [29], [38], [45], memory usage [45], data storage usage [45], packet delivery ratio [53], throughput [53], battery usage [38], and overhead cost [38], [53]. In terms of effectiveness, the system's ability to perform identity recognition is evaluated [22], [32], [44]. There are attempts to evaluate the usability of the system through questionnaires administered to users [29], [34]. These studies can reveal the user satisfaction and acceptance of the system, including whether they are satisfied with providing biometric information for authentication. There is a considerable focus on new multimodal biometric authentication technologies, but the number and scope of usability studies are limited. An analysis of user's satisfaction and acceptance provides the necessary information to improve the user's multibiometric authentication experience [67], but there is still a lack of in-depth discussion. Therefore, there is a requirement to further explore users' experiences on CMBA systems for successful practical deployment. Furthermore, it is crucial to consider the trade-off between security and usability to design the CMBA system by observing the window time for authentication, which is missing in the current knowledge body [29], [30].

E. NUMBER OF USERS AND DATASETS

The majority of the researchers surveyed use privately generated data from volunteers, while 26% of papers use public datasets (Fig. 7). The disadvantages of using a private dataset are: 1) most of the data is collected in a controlled environment (e.g., a specific task was given while collecting the data) and 2) the majority of the participants are university students or staff who are familiar with the use of the system. Therefore, such experiments may be irreproducible and unable to be used for further analysis by other interested researchers [12].

In papers surveyed, with the number of test users ranging from two users to six hundred users, Crawford, *et al.* [44] have the least number of users using virtual data to generate two virtual users to simulate a designed scenario (owner and attacker). In contrast, Monwar, *et al.* [25] have the largest number of users by combining a dataset attained from a public database. Murphy, *et al.* [26] have the highest number of users (103 participants) among the papers which use a private dataset and the longest data collection period (two and half years).

Many studies created a heterogeneous matrix (e.g., FAR, FRR, EER, FRM, etcetera) to evaluate the system's accuracy when considering performance evaluation. Even though accuracy measurement techniques vary amongst different papers, real usage statistics and measurement methodologies also differ. In addition, in terms of repeatability and true comparison of performance, performance across different systems evaluated would differ as most of the systems in papers surveyed are under bespoke, domain-specific control environments with short time durations used for predetermined tasks that are performed during the evaluation [1]. Ideally, for more robust comparisons and accurate insights in the reported performance for each CMBA system, extensible evaluation should be conducted with longer session times and interval sessions without artificial restrictions and constraints.

VI. FINDING AND DISCUSSION

This section summarizes and discusses the findings from section 5. To explore the design and evaluation approaches implemented in a CMBA system, a research question and five subcomponents are developed, and a systematic review is undertaken to explore these questions.

Research Question: How are continuous multimodal biometric authentication systems designed, implemented, and evaluated?

There is a large variability in the operational platforms that utilise a CMBA system. Broad platform types include computers (PC and laptop), mobile phones, wearable devices, IoT devices, and the network/communication infrastructure. This variation impacts the underlying authentication techniques that can be deployed thus subsequently the performance that can be achieved.

Multimodal biometrics authentication systems are proven to more secure than single modal biometrics authentication systems; however, there is no clear proven defining process on choosing which biometric traits are used in a system, and there is a lack of discussion on how many modalities should be used to optimise system performance. The literature surveyed does not consider using three or more biometric traits for CMBA systems possibly due to the complexity of the structure and feature matching process [68]. Using more than three modalities with adaptive mechanisms that consider localised criteria based on the local domain or specific platforms could open new areas of research in CMBA system.

Sub-Research Question 1: What are biometric cues used?

It is found that studies have employed a variety of biometric characteristics: behavioural only, physiological only and both, with soft biometrics (e.g., skin colour). Behavioural biometric combination is preferred in contrast to other combinations (physiological only or both) as it allows continuous and non-intrusive authentication mechanisms at low implementation cost. Comparative analysis between a single modal system and multimodal systems is very convincing that using multimodal biometrics provide more effective and accurate authentication systems; however, there are no comparative discussions in the studies that inform which combination of biometric types (e.g., fusion of behavioural and physiological cue vs fusion of behavioural cues only) is the most efficient and effective for a continuous authentication system. This further highlights the need for the comparative analysis between the different combination of biometric types.

Literature shows the possibility of various biometric types as authentication factors, but they have not fully addressed potential challenges of using selected biometric cues and what mitigations are needed to minimise the challenges. For example, surveyed literature reports of the challenges in face recognition such as illumination or angles [11], [34], [58], but they have not discussed the effects of aging. Additionally, fingerprint-based authentication is vulnerable to presentation attacks (the presentation of a fraudulent sample such as a fake biometric sample) [69], but there is no discussion in the literature as to how this can be detected and prevented in CMBA systems.

Authenticators of CMBA systems tend to be biased in selecting common biometric traits such as keystroke, face and fingerprints without considering further exploration on other biometric cues such as BVP, EGG or ECG signals. This is unfortunate as inclusion of these traits result in higher classification accuracy and efficiency [69], [70]. Therefore, detailed discussion on the vulnerabilities of biometric traits and remedies to minimise their impact on the overall system should be considered further. More exploration on various biometric traits is needed to give insight on how to choose the most appropriate biometric combinations based on the domain's application or purpose [71].

Sub-Research Question 2: What are classification algorithms used?

When considering the classification algorithm used, supervised machine learning algorithms (k-NN, NB, Random Forest) are more common and focused on continuous multimodal biometric authentication systems, as these algorithms tend to be more accurate than unsupervised learning techniques. Considering the limitations in supervised learning approaches (e.g., over-training issues), other machine learning approaches (unsupervised, semi-supervised) could have the potential to be used in continuous authentication systems; however, this potential has not been explored thoroughly – even though the efficacy of these approaches are recognized [30]. Therefore, more exploration of unsupervised learning and semi-supervised learning in continuous authentication systems is required.

Sub-Research Question 3: How are different modalities fused?

Score level fusion, which combines modality scores to form a single fused score, is most commonly used in CMBA systems due to convenience and simplicity. Even though there are comparative studies on system performance between score level fusion and feature level fusion, it is unclear whether score level fusion is better than feature level fusion. This is because the identified studies surveyed use different biometric traits and classification algorithms. The performance of the different fusion levels adopted could vary depending on the platform (e.g., mobile, wearable devices and more) and system architecture (e.g., biometric traits combined, and classification methods). Therefore, an exploration of the performance comparisons between different fusion levels under standardised, similar platforms and system architectures to gain insights into the best continuous authentication system's fusion method is warranted.

Sub-Research Question 4: What are the measures used to evaluate the performance of the authentication system?

Various metrics are used to evaluate the proposed CMBA systems. Most of the studies are focused on the evaluation of the system's recognition accuracy. FAR, FRR, and ERR are the predominant performance indicators used. As there is no unified standard to evaluate the accuracy of a biometric authentication system, it is very difficult to determine whether the system's performance indicators provide reliable results.

There are attempts to evaluate the security of a system under attack scenarios or threat models. However, the security evaluation scope is still limited as the reliability of a feature template and privacy implications of biometric data are neglected. Scalability and user acceptance and satisfaction are missing in most of the literature surveyed, even though these are important factors to ensure the system's feasibility under real-world deployments. Therefore, there is a need for future studies to explore scalability and usability, and in particular to include user acceptance and satisfaction measures.

Supervised machine learning algorithms require sufficient training data to achieve good classification results, but this can also result in overfitting [71]. As the most of the surveyed literature focuses on the recognition accuracy of CMBA systems, there is a lack of discussion on the effective training data size needed. The requirement of capturing supervised training data over a large time period could lower a user's satisfaction (and efficiency) experience; hence discussion on effective training data sizes and user experience should be explored in the future.

It is important to determine the window time of the authentication process in a CMBA system so that the system can ensure the accuracy of the authentication while optimising its operation costs [30]. However, the authentication window time is neglected in the majority of studies. Therefore, further evaluation to find effective observational window time should be considered to ensure the effectiveness of a CMBA system.

Sub-Research Question 5: What is the dataset used to evaluate the performance?

Private datasets are widely used to evaluate systems, but most of the data is collected under controlled, domain-specific environments, and the majority of the participants in the experiments are university students or staff. Therefore, a limitation is that the results obtained from these experiments could not reflect reality as they have an inherent selection bias (e.g., such participants may have higher IT skills or experience compared to other demographic groups). Additionally, the data is collected in short session durations; hence, it could not reflect whether the system can effectively and continuously authenticate users for long-term periods, especially if biometric data is used that can change over time (for example, face recognition). Therefore, it is necessary to conduct extensible evaluations with longer participation times under less-controlled/real-world environments to gain more accurate insights into these systems.

VII. CONCLUSION

Continuous multimodal biometric authentication (CMBA) systems promise more accurate and potentially less intrusive authentication mechanisms in contrast to single biometric authentication systems. We have analysed the current literature on CMBA systems to provide an insight on the state of the art on such systems and identify the corresponding research challenges and future directions. We expect this work can serve as a map to foster research advancements on the topic. Combining behavioural biometrics is preferred rather than physiological biometrics alone due to the low implementation cost and non-intrusive collection of such biometric data. As there is little or no discussion about system performance among the different combinations of biometric types (e.g. behavioural biometrics only, physiological biometrics only, or combination of behavioural and physiological biometrics), a comparative analysis of different biometric feature fusion techniques is worthy for further research. Indeed, the choice of biometric traits included in CMBA systems is still limited to common traits, and there is no broader exploration on inclusion of other biometrics such as ECG and BVG. Supervised machine learning techniques are the predominant classification techniques in CMBA systems. The choice of supervised and unsupervised machine learning is based on the training data volume and the use of specific authentication system. There are no comparative studies on the two approaches under the same multimodal biometric authentication system; hence it is still an open question of which method provides better performance for continuous authentication. Semi-supervised learning techniques are introduced, but studies using a semi-supervised learning algorithm are limited at present. Score level fusion is the most common and preferred fusion method due to its simplicity and adaptability. However, its performance has yet to be compared with other fusion levels (sample, feature and rank). CMBA systems' evaluation are focused on the accuracy of authentication; hence scalability, security, and usability of a system are revealed to have a lack of discussion in the literature even though these are crucial factors to determine the success of CMBA system implementation. The observational window time is crucial for a CMBA system as it impacts on usability and accuracy of the system [30], Therefore, more investigation is required to find acceptable window time for continuous authentication in practical applications, which is neglected in the most of the literature. Furthermore, these requirements should be evaluated extensively on real data to prove that CMBA systems are viable.

It is proven that systems that use continuous multimodal biometrics are more effective and secure than a system that employs a single modal biometric authentication system. However, there is no discussion with respect to system performance optimisation on the number of biometric traits adopted in the system. In future work, it would be beneficial to explore different biometric modalities (in particular consider three or more biometric modalities) and adaptively select different combinations of these biometric modalities depending on the authentication domain to improve the authentication system's usability and effectiveness.

This systematic review is believed to be comprehensive as it sources several leading publication databases, and it follows the Joanna Briggs Institute Reviewer's Manual [14] and PRISMA guideline [13]. However, the study focuses on continuous multimodal biometric authentication and articles written in English within a limited multi-year time period due to the requirement of narrowing scope and providing a comprehensive overview of the literature surveyed. It is possible that publications in other languages may have been omitted. Additionally, biometric authentication systems which may have been developed outside of this study's scope, such as static multimodal biometric systems or continuous unimodal biometric systems are omitted.

APPENDIX

See Table 6.

TABLE 6. List of thirty-nine (39) articles included in the systematic review.

Ref	Autor	Year	Paper Title
[19]	S. Acharya, A. Fridman, P. Brennan, P. Juola, R. Greenstadt, M. Kam and Ieee	2013	User Authentication Through Biometric Sensors and Decision Fusion
[31]	O. Aljohani, N. Aljohani, P. Bours and F. Alsolami	2018	Continuous Authentication on PCs using Artificial Immune System
[32]	S. Ayeswarya and J. Norman	2019	Improved usability for seamless user verification based on biometrics
[43]	C. Bo, L. Zhang, T. Jung, J. Han, X. Y. Li and Y. Wang	2015	Continuous user identification via touch and movement behavioral biometrics
[47]	K. Y. Chee, Z. Jin, W. S. Yap and B. M. Goi	2018	Two-dimensional winner-takes-all hashing in template protection based on fingerprint and voice feature level fusion
[44]	H. Crawford, K. Renaud and T. Storer	2013	A framework for continuous, transparent mobile device authentication
[20]	N. Damer, F. Maul, and C. Busch	2016	Multibiometric Continuous Authentication: a Trust Model for an Asynchronous System
[34]	M. De Marsico, C. Galdi, M. Nappi and D. Riccio	2014	FIRME: Face and Iris Recognition for Mobile Engagement
[52]	M. A. M. El-Bendary, H. Kasban, A. Haggag and M. A. R. El-Tokhy	2020	Investigating of nodes and personal authentications utilizing multimodal biometrics for medical application of WBANs security
[21]	L. Fridman, A. Stolerman, S. Acharya, P. Brennan, P. Juola, R. Greenstadt, M. Kam and F. Gomez	2015	Multimodal decision fusion for continuous authentication
[33]	M. Hammad, Y. Liu, K. Wang	2019	Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint
[35]	R. Kumar, V. V. Phoha and A. Serwadda	2016	Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns
[54]	B. Li, H. Sun, Y. Gao, V. V. Phoha and Z. Jin	2017	Enhanced free-text keystroke continuous authentication based on dynamics of wrist motion
[55]	B. Li, W. Wang, Y. Gao, V. V. Phoha and Z. Jin	2018	Hand in Motion: Enhanced authentication through wrist and mouse movement
[22]	M. Martinho, A. Fred and H. Silva	2018	Towards Continuous User Recognition by Exploring Physiological Multimodality: An Electrocardiogram (ECG) and Blood Volume Pulse (BVP) Approach
[23]	S. Mondal and P. Bours	2015	Context independent continuous authentication using behavioral biometrics
[24]	S. Mondal and P. Bours	2017	A study on continuous authentication using a combination of keystroke and mouse biometrics
[25]	M. M. Monwar, M. Gavrilova and Y. Wang	2011	A novel fuzzy multimodal information fusion technology for human biometric traits identification
[48]	T. M. Mostafa, I. A. El-Azab and N. F. El-Gayar	2012	Adaptive biometric verification system using quality-based co-training
[26]	C. Murphy, J. Huang, D. Hou and S. Schuckers	2018	Shared dataset on natural human-computer interaction to support continuous authentication research
[27]	R. Oak and M. Khare	2018	A Novel Architecture for Continuous Authentication using Behavioral Biometrics
[49]	A. Othman and A. Ross	2015	Fingerprint + Iris = IrisPrint
[56]	G. Peng, G. Zhou, D. T. Nguyen, X. Qi, Q. Yang and S. Q. Wang	2017	Continuous Authentication With Touch Behavioral Biometrics and Voice on Wearable Glasses
[28]	A. Prakash	2019	Continuous user authentication based score level fusion with hybrid optimisation
[45]	A. N. Putri, Y. D. W. Asnar and S. Akbar	2017	A continuous fusion authentication for Android based on keystroke dynamics and touch gesture
[36]	H. Saevanee, N. Clarke, S. Furnell and V. Biscione	2015	Continuous user authentication using multimodal biometrics
[37]	H. Saevanee, N. L. Clarke and S. M. Furnell	2012	Multimodal Behavioral Biometric Authentication for Mobile Devices
[50]	T. Sahayini and M. S. K. Manikandan	2016	Enhancing the security of modern ICT systems with multimodal biometric cryptosystem and continuous user authentication
[53]	M. Savitha and M. Senthilkumar	2020	A unique secure multimodal biometrics-based user authenticated key exchange protocol for generic HIoT networks
[29]	E. Schiavone, A. Ceccarelli, A. Carvalho and A. Bondavalli	2019	Design, implementation, and assessment of a usable multibiometric continuous authentication system
[30]	C. Shen, H. Zhang, Z. Yang and X. Guan	2017	Modeling multimodal biometric modalities for continuous user authentication

TABLE 6. ***(Continued.)*** **List of thirty-nine (39) articles included in the systematic review.**

[38]	D. M. Shila and K. Srivastava	2018	CASTRA: Seamless and Unobtrusive Authentication of Users to Diverse Mobile Services
[39]	M. Smith-Creasey and M. Rajarajan	2016	A continuous user authentication scheme for mobile devices
[40]	M. Smith-Creasey and M. Rajarajan	2019	A novel word-independent gesture-typing continuous authentication scheme for mobile devices
[7]	S. Srivastava and P. S. Sudhish	2017	Continuous multibiometric user authentication: Fusion of face recognition and keystoke dynamics
[46]	R. Vinothkanna and P. K. Sasikumar	2020	A novel multimodal biometrics system with fingerprint and gait recognition traits using contourlet derivative weighted rank fusion
[51]	M. Wang, H. A. Abbass, J. K. Hu and Ieee	2016	Continuous Authentication Using EEG and Face Images for Trusted Autonomous Systems
[41]	S. Wang, J. Yuan and S. Chen	2020	Quality-based score level fusion for continuous authentication with motion sensor and face
[42]	J. S. Wu, W. C. Lin, C. T. Lin and T. E. Wei	2016	Smartphone continuous authentication based on keystroke and gesture profiling

REFERENCES

[1] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and transparent multimodal authentication: Reviewing the state of the art," *Cluster Comput.*, vol. 19, no. 1, pp. 455–474, Mar. 2016, doi: 10.1007/s10586-015-0510-4.

[2] S. Ayeswarya and J. Norman, "A survey on different continuous authentication systems," *Int. J. Biometrics*, vol. 11, no. 1, p. 67, 2019, doi: 10.1504/IJBM.2019.096574.

[3] P. Arias-Cabarcos, C. Krupitzer, and C. Becker, "A survey on adaptive authentication," *ACM Comput. Surv.*, vol. 52, no. 4, pp. 1–30, Sep. 2019, doi: 10.1145/3336117.

[4] M. Singh, R. Singh, and A. Ross, "A comprehensive overview of biometric fusion," *Inf. Fusion*, vol. 52, pp. 187–205, Dec. 2019, doi: 10.1016/j.inffus.2018.12.003.

[5] I. C. Stylios, O. Thanou, I. Androulidakis, and E. Zaitseva, "A review of continuous authentication using behavioral biometrics," in *Proc. South-East Eur. Design Autom., Comput. Eng., Comput. Netw. Social Media Conf. SEEDA-CECNSM*, 2016, pp. 72–79, doi: 10.1145/2984393.2984403.

[6] 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, doi: 10.1016/j.patrec.2017.03.027.

[7] S. Srivastava and P. S. Sudhish, "Continuous multi-biometric user authentication fusion of face recognition and keystoke dynamics," in *Proc. IEEE Region 10 Humanitarian Technol. Conf. (R-HTC)*, Dec. 2016, pp. 1–7, doi: 10.1109/R10-HTC.2016.7906823. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85020221034&doi=10.1109%2fR10-HTC.2016.7906823&partnerID=40&md5=365b902476e5a5a57f167b16312caae7

[8] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1268–1293, 3rd Quart., 2015, doi: 10.1109/COMST.2014.2386915.

[9] R. Ouch, B. Garcia-Zapirain, and R. Yampolskiy, "Multimodal biometrie systems: A systematic review," in *Proc. IEEE Int. Symp. Signal Process. Inf. Technol. (ISSPIT)*, Dec. 2017, pp. 439–444, doi: 10.1109/ISSPIT.2017.8388683.

[10] R. Gad, N. El-Fishawy, A. EL-SAYED, and M. Zorkany, "Multi-biometric systems: A state of the art survey and research directions," *Int. J. Adv. Comput. Sci. Appl.*, vol. 6, no. 6, pp. 128–138, 2015, doi: 10.14569/IJACSA.2015.060618.

[11] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Syst. Appl.*, vol. 143, Apr. 2020, Art. no. 113114, doi: 10.1016/j.eswa.2019.113114.

[12] A. Ekpezu, E. Umoh, F. Koranteng, and J. Abandoh-Sam, "Biometric authentication schemes and methods on mobile devices: A systematic review," in *Modern Theories and Practices for Cyber Ethics and Security Compliance*, W. Yaokumah, M. Rajarajan, J.-D. Abdulai, I. Wiafe, and F. A. Katsriku, Eds. Hershey, PA, USA: IGI Global, 2020.

[13] L. A. D. Moher, J. Tetzlaff, A. DG, and T. P. Group, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *PLoS Med.*, vol. 6, no. 7, 2009, Art. no. e1000097, doi: 10.1371/journal.pmed.1000097.

[14] The Joanna Briggs Institute. (2014). *Joanna Briggs Institute Reviewers' Manual: 2014 Edition/ Supplement*. The Joanna Briggs Institute, Australia. [Online]. Available: https://nursing.lsuhsc.edu/JBI/docs/ReviewersManuals/Economic.pdf

[15] *IEEE Xplore*. Accessed: Aug. 1, 2020. [Online]. Available: https://ieeexplore-ieee-org.ezproxy.utas.edu.au/Xplore/home.jsp

[16] *Science Direct*. Accessed: Aug. 1, 2020. [Online]. Available: https://www-sciencedirect-com.ezproxy.utas.edu.au/search

[17] *Scopus*. Accessed: Aug. 1, 2020. [Online]. Available: https://www-scopus-com.ezproxy.utas.edu.au/search/form.uri?display=basic#basic

[18] *Web of Science*. Accessed: Aug. 1, 2020. [Online]. Available: https://apps-webofknowledge-com.ezproxy.utas.edu.au/WOS_GeneralSearch_input.do?product=WOS&search_mode=GeneralSearch&SID=C18LsDiDWkTb7Dldu1v&preferencesSaved=

[19] S. Acharya, A. Fridman, P. Brennan, P. Juola, R. Greenstadt, and M. Kam, "User authentication through biometric sensors and decision fusion," in *Proc. 47th Annu. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2013, pp. 1–6.

[20] N. Damer, F. Maul, and C. Busch, "Multi-biometric continuous authentication: A trust model for an asynchronous system," *Proc. 19th Int. Conf. Inf. Fusion)*. New York, NY, USA, Jul. 2016, pp. 2192–2199.

[21] L. Fridman, A. Stolerman, S. Acharya, P. Brennan, P. Juola, R. Greenstadt, and M. Kam, "Multi-modal decision fusion for continuous authentication," *Comput. Electr. Eng.*, vol. 41, pp. 142–156, Jan. 2015, doi: 10.1016/j.compeleceng.2014.10.018.

[22] M. Martinho, A. Fred, and H. Silva, "Towards continuous user recognition by exploring physiological multimodality: An electrocardiogram (ECG) and blood volume pulse (BVP) approach," in *Proc. Int. Symp. Sens. Instrum. IoT Era (ISSI)*, Sep. 2018, pp. 1–6, doi: 10.1109/ISSI.2018.8538075. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85059361399&doi=10.1109%2fISSI.2018.8538075&partnerID=40&md5=fdeab191dded39d3c66947a2b5e75118

[23] S. Mondal and P. Bours, "Context independent continuous authentication using behavioural biometrics," in *Proc. IEEE Int. Conf. Identity, Secur. Behav. Anal. (ISBA)*, Mar. 2015, pp. 1–8, doi: 10.1109/ISBA.2015.7126342.

[24] S. Mondal and P. Bours, "A study on continuous authentication using a combination of keystroke and mouse biometrics," *Neurocomputing*, vol. 230, pp. 1–22, Mar. 2017, doi: 10.1016/j.neucom.2016.11.031.

[25] M. M. Monwar, M. Gavrilova, and Y. Wang, "A novel fuzzy multimodal information fusion technology for human biometric traits identification," in *Proc. IEEE 10th Int. Conf. Cognit. Informat. Cognit. Comput. (ICCI-CC)*, Aug. 2011, pp. 112–119, doi: 10.1109/COGINF.2011.6016128.

[26] C. Murphy, J. Huang, D. Hou, and S. Schuckers, "Shared dataset on natural human-computer interaction to support continuous authentication research," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2017, pp. 528–530, doi: 10.1109/BTAS.2017.8272738. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046289912&doi=10.1109%2fBTAS.2017.8272738&partnerID=40&md5=3c385056cbdffecf59ec4b81ff7ea4fc

[27] R. Oak and M. Khare, "A novel architecture for continuous authentication using behavioural biometrics," in *Proc. Int. Conf. Current Trends Comput., Electr., Electron. Commun. (CTCEEC)*, Sep. 2017, pp. 767–771, doi: 10.1109/CTCEEC.2017.8455040. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054083352&doi=10.1109%2fCTCEEC.2017.8455040&partnerID=40&md5=8907f114e67cbd38d917d55a81af37e7

[28] A. Prakash, "Continuous user authentication based score level fusion with hybrid optimization," *Cluster Comput.*, vol. 22, no. S5, pp. 12959–12969, Sep. 2019, doi: 10.1007/s10586-018-1819-6.

[29] E. Schiavone, A. Ceccarelli, A. Carvalho, and A. Bondavalli, "Design, implementation, and assessment of a usable multi-biometric continuous authentication system," *Int. J. Crit. Comput.-Based Syst.*, vol. 9, no. 3, pp. 215–247, 2019, doi: 10.1504/IJCCBS.2019.104490.

[30] C. Shen, H. Zhang, Z. Yang, and X. Guan, "Modeling multimodal biometric modalities for continuous user authentication," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2016, pp. 1894–1899, doi: 10.1109/SMC.2016.7844515. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85015728416&doi=10.1109%2fSMC.2016.7844515&partnerID=40&md5=a3cfbdc0193cccba57ba83b671fdca35

[31] O. Aljohani, N. Aljohani, P. Bours, and F. Alsolami, "Continuous authentication on PCs using artificial immune system," in *Proc. 1st Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Apr. 2018, pp. 1–6, doi: 10.1109/CAIS.2018.8442022.

[32] S. Ayeswarya and J. Norman, "Improved usability for seamless user verification based on biometrics," *Int. J. Adv. Sci. Technol.*, vol. 28, no. 7, pp. 379–391, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85080134497&partnerID=40&md5=7cee76ec9da5accdd2fc24863efbd901

[33] M. Hammad, Y. Liu, and K. Wang, "Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint," *IEEE Access*, vol. 7, pp. 26527–26542, 2019, doi: 10.1109/ACCESS.2018.2886573.

[34] M. De Marsico, C. Galdi, M. Nappi, and D. Riccio, "FIRME: Face and iris recognition for mobile engagement," *Image Vis. Comput.*, vol. 32, no. 12, pp. 1161–1172, Dec. 2014, doi: 10.1016/j.imavis.2013.12.014.

[35] R. Kumar, V. V. Phoha, and A. Serwadda, "Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns," in *Proc. IEEE 8th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Sep. 2016, pp. 1–8, doi: 10.1109/BTAS.2016.7791164.

[36] H. Saevanee, N. Clarke, S. Furnell, and V. Biscione, "Continuous user authentication using multi-modal biometrics," *Comput. Secur.*, vol. 53, pp. 234–246, Sep. 2015, doi: 10.1016/j.cose.2015.06.001.

[37] H. Saevanee, N. L. Clarke, and S. M. Furnell, "Multi-modal behavioural biometric authentication for mobile devices," in *Information Security and Privacy Research* (IFIP Advances in Information and Communication Technology), vol. 376, D. Gritzalis, S. Furnell, and M. Theoharidou, Eds. Berlin, Germany: Springer, 2012, pp. 465–474.

[38] D. M. Shila and K. Srivastava, "CASTRA: Seamless and unobtrusive authentication of users to diverse mobile services," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 4042–4057, Oct. 2018, doi: 10.1109/JIOT.2018.2851501.

[39] M. Smith-Creasey and M. Rajarajan, "A continuous user authentication scheme for mobile devices," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, Dec. 2016, pp. 104–113, doi: 10.1109/PST.2016.7906944. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85019223601&doi=10.1109%2fPST.2016.7906944&partnerID=40&md5=edba9ca8f36f78a96dc292f4e99e9953

[40] M. Smith-Creasey and M. Rajarajan, "A novel word-independent gesture-typing continuous authentication scheme for mobile devices," *Comput. Secur.*, vol. 83, pp. 140–150, Jun. 2019, doi: 10.1016/j.cose.2019.02.001.

[41] S. Wang, J. Yuan, and S. Chen, "Quality-based score level fusion for continuous authentication with motion sensor and face," in *Proc. 4th Int. Conf. Cryptogr., Secur. Privacy*, Jan. 2020, pp. 58–62, doi: 10.1145/3377644.3377647. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85081123194&doi=10.1145%2f3377644.3377647&partnerID=40&md5=977a46216ed739637351e367490e7d5b

[42] J.-S. Wu, W.-C. Lin, C.-T. Lin, and T.-E. Wei, "Smartphone continuous authentication based on keystroke and gesture profiling," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Sep. 2015, pp. 191–197, doi: 10.1109/CCST.2015.7389681. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84964811142&doi=10.1109%2fCCST.2015.7389681&partnerID=40&md5=56780b42682ef66d3106611d106ba588

[43] C. Bo, L. Zhang, T. Jung, J. Han, X.-Y. Li, and Y. Wang, "Continuous user identification via touch and movement behavioral biometrics," in *Proc. IEEE 33rd Int. Perform. Comput. Commun. Conf. (IPCCC)*, Dec. 2014, doi: 10.1109/PCCC.2014.7017067. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84923169190&doi=10.1109%2fPCCC.2014.7017067&partnerID=40&md5=474c1d9fc7017a0ba06882fdd61af654

[44] H. Crawford, K. Renaud, and T. Storer, "A framework for continuous, transparent mobile device authentication," *Comput. Secur.*, vol. 39, pp. 127–136, Nov. 2013, doi: 10.1016/j.cose.2013.05.005.

[45] A. N. Putri, Y. D. W. Asnar, and S. Akbar, "A continuous fusion authentication for Android based on keystroke dynamics and touch gesture," in *Proc. Int. Conf. Data Softw. Eng. (ICoDSE)*, Oct. 2016, pp. 1–6, doi: 10.1109/ICODSE.2016.7936146. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85025585889&doi=10.1109%2fICODSE.2016.7936146&partnerID=40&md5=d70ee698376e0dadf9e97c35a828f722

[46] R. Vinothkanna and P. K. Sasikumar, "A novel multimodal biometrics system with fingerprint and gait recognition traits using contourlet derivative weighted rank fusion," in *Computational Vision and Bio-Inspired Computing* (Advances in Intelligent Systems and Computing), vol. 1108. Hong Kong: IEEE Press, 2020, pp. 950–963.

[47] K.-Y. Chee, Z. Jin, W.-S. Yap, and B.-M. Goi, "Two-dimensional winner-takes-all hashing in template protection based on fingerprint and voice feature level fusion," in *Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA ASC)*, Dec. 2017, pp. 1411–1419, doi: 10.1109/APSIPA.2017.8282253. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046796139&doi=10.1109%2fAPSIPA.2017.8282253&partnerID=40&md5=b4e7d31e41c73db8fcaf1b8d94af6b43

[48] T. M. Mostafa, I. A. El-Azab, and N. F. El-Gayar, "Adaptive biometric verification system using quality-based co-training," in *Proc. 11th Int. Conf. Inf. Sci., Signal Process. Their Appl. (ISSPA)*, Jul. 2012, pp. 1313–1318, doi: 10.1109/ISSPA.2012.6310496.

[49] A. Othman and A. Ross, "Fingerprint + Iris = IrisPrint," *Proc. SPIE*, vol. 2015, vol. 9457, Art. no. 945703, doi: 10.1117/12.2181075. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84948689662&doi=10.1117%2f12.2181075&partnerID=40&md5=99aa7e7820945e79900ee0fde04fd92e

[50] T. Sahayini and M. S. K. Manikandan, "Enhancing the security of modern ICT systems with multimodal biometric cryptosystem and continuous user authentication," *Int. J. Inf. Comput. Secur.*, vol. 8, no. 1, pp. 55–71, 2016, doi: 10.1504/IJICS.2016.075310.

[51] M. Wang, H. A. Abbass, and J. Hu, "Continuous authentication using EEG and face images for trusted autonomous systems," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, Dec. 2016, pp. 368–375.

[52] M. A. M. El-Bendary, H. Kasban, A. Haggag, and M. A. R. El-Tokhy, "Investigating of nodes and personal authentications utilizing multimodal biometrics for medical application of WBANs security," *Multimedia Tools Appl.*, vol. 79, nos. 33–34, pp. 24507–24535, Sep. 2020, doi: 10.1007/s11042-020-08926-2.

[53] S. M, "A unique secure multimodal biometrics-based user authenticated key exchange protocol for generic HIoT networks," *Int. J. Emerg. Trends Eng. Res.*, vol. 8, no. 5, pp. 1610–1619, May 2020, doi: 10.30534/ijeter/2020/22852020.

[54] B. Li, H. Sun, Y. Gao, V. V. Phoha, and Z. Jin, "Enhanced free-text keystroke continuous authentication based on dynamics of wrist motion," in *Proc. IEEE Workshop Inf. Forensics Secur., WIFS*, Jan. 2018, pp. 1–6, doi: 10.1109/WIFS.2017.8267642. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85049797604&doi=10.1109%2fWIFS.2017.8267642&partnerID=40&md5=227957349a54e6a04c89fa15e068f505

[55] B. Li, W. Wang, Y. Gao, V. V. Phoha, and Z. Jin, "Hand in motion: Enhanced authentication through wrist and mouse movement," in *Proc. IEEE 9th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Oct. 2018, doi: 10.1109/BTAS.2018.8698577. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85065430731&doi=10.1109%2fBTAS.2018.8698577&partnerID=40&md5=a4f4308c5900de652242e63085aa57b2

[56] G. Peng, G. Zhou, D. T. Nguyen, X. Qi, Q. Yang, and S. Wang, "Continuous authentication with touch behavioral biometrics and voice on wearable glasses," *IEEE Trans. Human-Mach. Syst.*, vol. 47, no. 3, pp. 404–416, Jun. 2017, doi: 10.1109/thms.2016.2623562.

[57] M.-G. Kim, H.-M. Moon, Y. Chung, and S. B. Pan, "A survey and proposed framework on the soft biometrics technique for human identification in intelligent video surveillance system," *J. Biomed. Biotechnol.*, vol. 2012, Jul. 2012, Art. no. 614146, doi: 10.1155/2012/614146.

[58] K. Guo, S. Wu, and Y. Xu, "Face recognition using both visible light image and near-infrared image and a deep network," *CAAI Trans. Intell. Technol.*, vol. 2, no. 1, pp. 39–47, Mar. 2017, doi: 10.1016/j.trit.2017.03.001.

[59] H. Fang, X. Wang, and S. Tomasin, "Machine learning for intelligent authentication in 5G and beyond wireless networks," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 55–61, Oct. 2019, doi: 10.1109/MWC.001.1900054.

[60] A. Mian, "Unsupervised learning from local features for video-based face recognition," in *Proc. 8th IEEE Int. Conf. Autom. Face Gesture Recognit.*, Sep. 2008, pp. 1–6, doi: 10.1109/AFGR.2008.4813310.

[61] P. Chaovalit and L. Zhou, "Movie review mining: A comparison between supervised and unsupervised classification approaches," in *Proc. 38th Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2005, p. 112, doi: 10.1109/HICSS.2005.445.

[62] G. F. Ling, P. Y. Han, K. E. Yee, and O. S. Yin, "Face recognition via semi-supervised discriminant local analysis," in *Proc. IEEE Int. Conf. Signal Image Process. Appl. (ICSIPA)*, Oct. 2015, pp. 292–297, doi: 10.1109/ICSIPA.2015.7412207.

[63] A. Ross and N. Poh, Eds. "Multibiometric systems: Overview, case studies, and open issues," in *Handbook of Remote Biometrics*. London, U.K.: Springer, 2009.

[64] Y. Sutcu, H. T. Sencar, and N. Memon, "A secure biometric authentication scheme based on robust hashing," in *Proc. 7th Workshop Multimedia Secur. - MM&Sec*, 2005, doi: 10.1145/1073170.1073191.

[65] A. B. Bondi, "Characteristics of scalability and their impact on performance," presented at the Proc. 2nd Int. Workshop Softw. Perform., Ottawa, ON, Canada, 2000, doi: 10.1145/350391.350432.

[66] L. M. Mayron, Y. Hausawi, G. S. Bahr, Eds., "Secure, usable biometric authentication systems," in *Universal Access in Human-Computer Interaction. Design Methods, Tools, and Interaction Techniques for eInclusion* (Lecture Notes in Computer Science) Berlin, Germany: Springer, 2013, pp. 195–204.

[67] M. El-Abed, R. Giot, B. Hemery, and C. Rosenberger, "A study of users' acceptance and satisfaction of biometric systems," in *Proc. 44th Annu. IEEE Int. Carnahan Conf. Secur. Technol.*, Oct. 2010, pp. 170–178, doi: 10.1109/CCST.2010.5678678.

[68] M. S. El_Tokhy, "Robust multimodal biometric authentication algorithms using fingerprint, iris and voice features fusion," *J. Intell. Fuzzy Syst.*, vol. 40, no. 1, pp. 647–672, Jan. 2021, doi: 10.3233/JIFS-200425.

[69] R. M. Jomaa, H. Mathkour, Y. Bazi, and M. S. Islam, "End-to-end deep learning fusion of fingerprint and electrocardiogram signals for presentation attack detection," *Sensors*, vol. 20, no. 7, p. 2085, Apr. 2020, doi: 10.3390/s20072085.

[70] M. Hammad and K. Wang, "Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network," *Comput. Secur.*, vol. 81, pp. 107–122, Mar. 2019, doi: 10.1016/j.cose.2018.11.003.

[71] X. Zhang, D. Cheng, P. Jia, Y. Dai, and X. Xu, "An efficient Android-based multimodal biometric authentication system with face and voice," *IEEE Access*, vol. 8, pp. 102757–102772, 2020, doi: 10.1109/ACCESS.2020.2999115.

RISEUL RYU was born in South Korea, in 1990. She received the Bachelor of Economics, the Master of Professional Accounting, and the Master of Information Technology and Systems degrees from the University of Tasmania, Australia, in 2012, 2015, and 2019, respectively.

From 2015 to 2018, she was an Accountant with Air Liquide Company Ltd., Seoul, South Korea. Since 2019, she has been a Casual Academic Staff with the Discipline of ICT, University of Tasmania, Australia. Her research interests include development and application of cybersecurity software using machine learning, and blockchain technology with the Internet of Things.

SOONJA YEOM (Member, IEEE) was born in South Korea, in 1964. She received the master's degree in computing and the Ph.D. degree from the University of Tasmania, Australia, in 1994 and 2017, respectively.

Since 1994, she has been a Lecturer with the School of Computing, Hobart University of Tasmania. Her research interests include big data, cyber security, affective computing, and educational technology.

SOO-HYUNG KIM (Member, IEEE) received the B.S. degree in computer engineering from Seoul National University, in 1986, and the M.S. and Ph.D. degrees in computer science from the Korea Advanced Institute of Science and Technology, in 1988 and 1993, respectively.

Since 1997, he has been a Professor with the School of Electronics and Computer Engineering, Chonnam National University, South Korea. His research interests include pattern recognition, document image processing, medical image processing, and deep learning.

DAVID HERBERT was born in Tasmania, in 1970. He received the Bachelor of Science degree, in 1991, followed by Honours, in 1992, and the Ph.D. degree in artificial intelligence from the University of Tasmania, Hobart, in 2020. From 1997 to 2016, he was a Senior Technical Officer and a Casual Lecturer with the School of Computing, University of Tasmania. His research interests include knowledge base systems, natural language processing, embedded systems, robotics, and cyber security.