Deep Learning in Biometric Authentication: Challenges, Recent Advancements, and Future Trends

Abdullah Alduhailan [1,*], Nazhatul Hafizah Kamarudin [1], Siti Norul Huda Sheikh Abdullah [1], and Aminu Dau [2]

[1] Centre for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Malaysia
[2] Department of Computer Science, Hassan Usman Katsina Polytechnic, Katsina, Nigeria
Email: Mazd794_3@hotmail.com (A.A.); nazhatulhafizah@ukm.edu.my (N.H.K.); snshabdullah@ukm.edu.my (S.N.H.S.A.); dauaminu@gmail.com (A.D.)
*Corresponding author

***Abstract*—Biometric systems have significantly improved with the integration of machine learning, especially with deep learning methods. As technology advances, it presents both new security risks and chances for biometrics to be used in a variety of contexts. Due to their remarkable success, recently, deep learning-based biometric methods have seen a dramatic increase in research papers. Thus, to compile and analyze research publications in the field, this paper presents a systematic a Systematic Literature Review (SLR). The review adopts the Systematic Reviews and Meta-Analyses (PRISMA) approach for the collection, analysis, and reporting of findings from relevant research. For this study, 109 papers in all were chosen from top digital libraries using predetermined search criteria. The most popular deep learning approaches in these systems, important biometric authentication strategies, and commonly used assessment metrics are highlighted in the review. Finally, the main challenges with deep learning-based biometric authentication methods are outlined in the paper, along with possible future trends in the field.**

***Keywords*—biometrics, authentication, biometric recognition, Deep Learning (DL), artificial neural network**

I. Introduction

Biometric technology encompasses the use of unique personal characteristics for identification, such as voice recognition, fingerprint recognition, facial recognition, etc. [1, 2]. As a dependable and secure approach to access control that provides individualized authentication and identity, biometrics has received a great deal of popularity [3, 4]. The main reason for the widespread adoption of biometric solutions is that they allow users to authenticate themselves while gaining access to systems or services. Biometric techniques have gradually replaced traditional authentication mechanisms like passwords [5]. Because biometric authentication ensures the protection of sensitive data and transactions, it has been widely adopted in industries such as government, healthcare, and finance [6]. The use of biometric authentication is becoming more widely accepted as a reliable solution to security issues [7]. An individual's distinct physiological or behavioral characteristics can be used to identify them, ensuring secure and effective authentication procedures. The integration of Machine Learning (ML) within biometric authentication frameworks has consistently improved the precision and efficacy of biometric capture technologies [8]. Traditional machine learning-driven biometric recognition tasks still face several challenges, nevertheless.

For instance, characteristics that have been hand-picked to work well for one biometric modality might not work as well for another [7]. Deep learning architectures offer a holistic learning paradigm capable of simultaneously learning feature representations and performing classification tasks [9]. As a result of the successful implementations of deep learning techniques in biometric recognition, there has been a notable surge in research publications centered around these techniques [9, 10]. For future researchers and practitioners in this field, this circumstance emphasizes the need for a comprehensive evaluation and synthesis of the existing literature in order to promote improved understanding and insight. In order to thoroughly assess the present corpus of research in the field of deep learning-based biometric detection, the goal of this work is to do a systematic literature review.

The Systematic Literature Review (SLR) in this study will focus on deep learning approaches for biometric authentication in particular. We will focus on research done from 2018 to 2024 to showcase the most recent developments in deep learning-based biometric authentication. The study will provide insightful information about current contributions, challenges, and emerging trends in this field, establishing the framework for future research and innovative developments. Here is a summary of this paper's main contributions:

Manuscript received October 24, 2024; revised November 12, 2024; accepted December 31, 2024; published April 9, 2025.

- Summarizing the most popular biometric authentication methods that utilize DL-based algorithms.
- Identifying the DL-based techniques applied to address biometric authentication tasks.
- Exploring the most widely used assessment criteria in deep learning-based biometric authentication approaches.
- Investigating the research challenges faced by deep learning-based biometric authentication.

The article is organized as follows in the remaining sections: In Section II, pertinent surveys in the realm of biometric authentication are reviewed. The approach for the review is presented in Section III. The summarized results are shown in Section IV. The paper's conclusions are finally summed up in Section V.

II. Related Reviews

The use of biometrics as a dependable approach to access control has gained popularity recently as a means of enhancing accessibility and security through the application of various ML approaches. Yang *et al.*'s work [11] goes into great detail about how biometrics might be used to improve security, specifically with regard to encoding and authentication. It offers insightful information about the current status of cryptographic and biometric-based authentication systems. An overview of soft biometric characteristics is provided by Tomicic *et al*. [12], who look at a range of variables such as physical, behavioral, and environmental aspects. In a similar vein, Gayathri *et al*. [13] provide a thorough analysis of several biometric methods and their uses.

Although Junaid *et al.*'s study [14] focuses on the combination of sensors and vital health indicators, it does not offer a comprehensive systematic analysis or much coverage of additional biometric domains. While their research does not cover other biometric modalities, Khoirunnisaa *et al*. [15] focus on iris-based biometric systems. A thorough analysis of AI-powered sensors for Internet of Things applications is given by Mukhopadhyay *et al*. [16]. Furthermore, Ross *et al*. [17] explore digital forensic systems for biometric data in smart cities; however, they do not discuss the integration of deep learning models with biometric security or the broader scope of biometric security.

The review by Karthik *et al*. [18] discusses the difficulties in utilizing the Internet of Things (IoT) with biomedical instruments; however, this work does not provide a thorough examination of biometric authentication methods. Similarly, Mariani *et al*. [19] present a comparable study that explores the impact of biometrics on ensuring security, as well as how AI can enhance biometric security functionalities.

The sensors used, the variety of applications, and the possible difficulties associated with the integration of IoT technology in apparel and textiles are examined by the authors in reference [19]. On the other hand, Liang *et al*. [20] tackle the ever-changing problems with user identification, stressing the significance of constant observation and the examination of distinct behavioral patterns exhibited by people.

Although each of the review articles in this part examines a different facet of biometric authentication, they all have significant drawbacks. These limitations include the narrow scope of the reviewed articles, which restricts comprehensive synthesis and analysis, and the omission of other subdomains within deep learning-based biometrics. Furthermore, current methods fail to thoroughly explore critical challenges and emerging trends in the field, leaving significant gaps in understanding and advancement. As a result, our study is notable for being unique and pertinent. In order to perform a comprehensive Systematic Literature Review (SLR), we will identify the most popular deep learning-based biometric authentication techniques, summarize them, look at evaluation standards, and assess the main obstacles and potential paths forward in this field.

III. Research Method

The research methodology is essential for any research endeavor. The methodology we used to carry out the SLR is described in this section. Our research complies with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) criteria [21]. A useful and repeatable framework for locating, picking, and evaluating recent research is provided by PRISMA. It also offers recommendations on how to identify, select, and assess the studies. Fig. 1 shows the primary steps of the review.

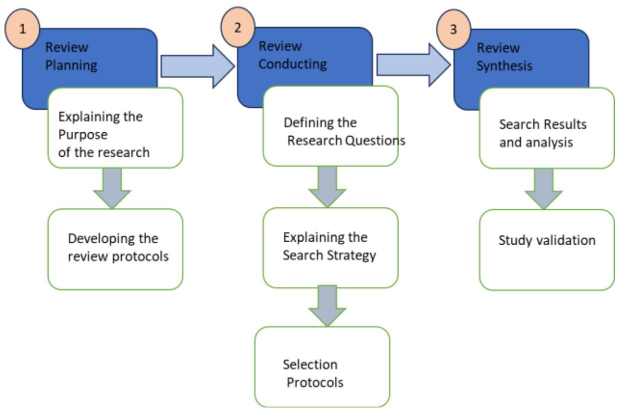

Fig. 1. Overview of stages of the SLR.

A. Review Planning

The planning step outlines the SLR's conception and preparation procedures, which include determining the study's objective and designing the review protocol. In order to find more relevant publications for the SLR, an automatic search was done on the main relevant digital databases. The relevant digital libraries we used include Scopus, Web of Science, IEEE Xplore library, SpringerLink, ScienceDirect, and ACM Digital. The years 2018 to 2024 were taken into consideration for the review in order to acquire the most recent and thorough systematic review. These libraries were taken into consideration because of their well-known status and abundance of literature relevant to the study. Table I shows the relevant databases with their corresponding links.

TABLE I. DIGITAL LIBRARY DATABASES

Database	Website
Science Direct	https://www.sciencedirect.com
SpringerLink	https://link.springer.com
ACM Digital Library	https://dl.acm.org
IEEE Explore	https://ieeexplore.ieee.org
Scopus	https://www.scopus.com
Web of Science	https://www.webofscience.com/wos

B. *Review Conducting*

Following the planning of the review, the next step is to execute it. During this phase, the core review process takes place, which includes specifying the Research Questions (RQs) for the systematic literature review. These RQs guide the exploration and address key topics related to biometric authentication. Furthermore, the steps for selecting a search strategy, as well as for extracting and synthesizing data, are discussed at this point. Thus, to realize the primary goal of the review, we put forward the RQs as given in Table II.

TABLE II. RESEARCH QUESTIONS (RQS)

Research question	Purpose
What are the popular domains that use biometric authentication?	To identify the most popular domains that apply biometric authentication.
What is the common deep learning-based Biometric authentication?	To identify the commonly used deep learning methods for biometric authentication
What are the popular deep learning algorithms used for biometric authentication?	To identify the deep learning algorithms for biometric authentication.
What are the most used evaluation metrics for biometric authentication?	To find the most popular evaluation metric used for biometric authentication.
What are the research challenges in deep learning-based biometric authentication?	To identify the research challenges in the field.
What are the future trends of biometric authentication?	To investigate the future trend in the biometric authentication field.

1) *Search strategy*

To gather more relevant studies, we develop certain search strings that are pertinent to the research questions of this review. This entails employing Boolean terms, like "OR" "AND," to combine search strings that are pertinent to the research questions of this review. The search string used for the SLR consists of ("Biometric Authentication" OR "Biometrics Recognition") AND ("Artificial Neural Network" OR "Deep Learning") AND ("Artificial Neural Network" AND "Authentication") AND ("Detection techniques" OR "Biometric recognition") AND ("Biometric Authentication Domain"). With each search for a digital library, the search terms are changed and transformed into the proper input requests.

2) *Selection protocol*

Fig. 2 shows the research article selection procedure and the technique applied to the selection of the papers in this review. To fully find the pertinent articles, we carried out a manual search in addition to the search phrase used in the automated search. Following the PRISMA guideline [21], in the identification stage, a total of 1866 studies were obtained. In the screening stage, after filtering duplicate, unsuitable, and irrelevant papers and after going through the abstract, introduction, and title, 542 published studies were eliminated. Thereafter, 377 research articles were moved to the next stage. In the eligibility phase, 268 research articles were eliminated after the evaluation of whole papers. Finally, 109 publications were chosen for the review after following the inclusion/exclusion strategy as well as the quality assessment. The exclusion/inclusion criteria used for the research article selection are mentioned in Table III.

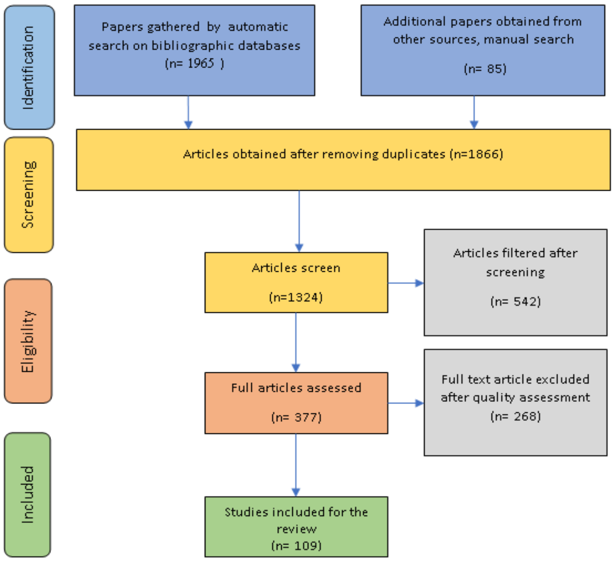

Fig. 2. The PRISM selection process of the SLR.

TABLE III. INCLUSION/EXCLUSION CRITERIA

Criteria	Inclusion	Exclusion
Study Type	Only Research works involving experimental results were considered.	Research works without experimental results were excluded.
Language	Only Articles written in English were used.	Articles written in other languages were not considered.
Year	Only Research works published from 2018 to 2024 were considered.	Research works published before 2018 were not considered.
Scope	Only papers focused on deep learning-based biometrics were considered.	Papers focus on other techniques used for biometrics not considered.
Source	Only conferences and journals were considered for the review.	Other sources such as the thesis, books, and magazines were not considered.

IV. SEARCH RESULTS AND SYNTHESIS

In this section, we present the search results and synthesis of the SLR. We first provide the description of the selected papers used for the SLR and then present answers to the RQs stated in the previous section.

A. *Description of the Studies*

This section presents the description of the articles considered for this SLR after the search and selection criteria. Publications on the deep learning-based biometrics authentication techniques found in the SLR from 2018 to 2024 are plotted in Fig. 3. The studies utilized in this SLR are shown chronologically in this visual form. Research activity has increased noticeably in recent years, especially since a specific moment in time, according to the data from the figure. It is evident that most of the publications included in this study were released before 2019. It is noteworthy that 2022 had the most publications (22), with 2020 and 2023 following closely behind with 19 articles. 2018 and 2019 saw 13 and 15 articles, respectively.

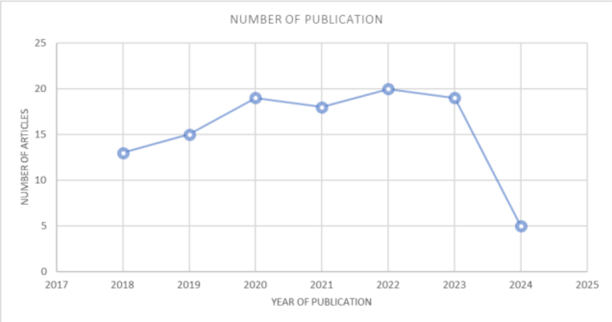

Fig. 3. Number of articles reviewed and the year of publication.

Fig. 4 presents a breakdown of the article categorization consisting of either journal articles, conference articles, or workshop articles. From the figure, one can see that the majority of the articles included in the review were from journals (54%) followed by the conference articles (29%) and the workshop articles (17%). We also identified the number of articles obtained from different bibliographic libraries, as illustrated in Fig. 5. As stated earlier, six different bibliographic databases were used to search for articles for the SLR. These databases include Scopus, Science Direct, SpringerLink, IEEE Xplore, Web of Science, and the ACM Digital Library.

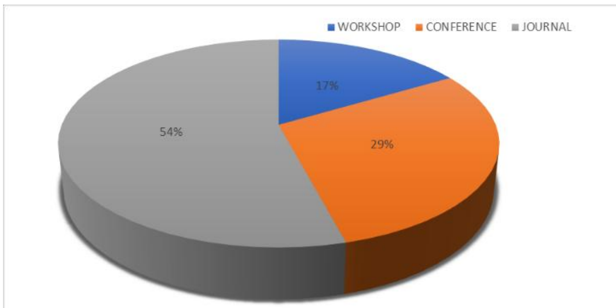

Fig. 4. Types of the articles used in the review.

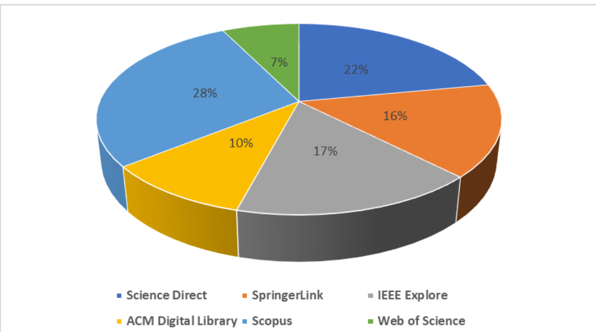

Fig. 5. Distribution of the articles in the digital libraries.

It is clear from the statistics in Fig. 5 that the two sources that supplied the most articles were Scopus and Science Direct, which accounted for 28% and 22% of all articles, respectively. These were followed by publications from IEEE Xplore (17%) and SpringerLink (17%). With 10% and 7% of the total articles, respectively, the ACM Digital Library and Web of Science made the fewest contributions. This distribution demonstrates how different these databases are in terms of coverage and applicability to our particular research question. The fact that the majority of the papers were from Science Direct and Scopus indicates that these databases are especially valuable resources for the area being studied. Conversely, the lesser contributions from Web of Science and the ACM Digital Library suggest either a smaller number of pertinent publications in these databases or possibly a more limited focus that does not directly match our study requirements.

B. RQ1: What Are the Applications Domainsn of the Biometricss Authentication?

The purpose of this section is to address RQ1. There are various application domains for biometrics authentication, according to the reviewed articles in the literature. These comprise cloud and fog computing [22–24], smart IoT, health [25–27], industry [28, 29], and communication. The main emphasis is on how authorization frameworks are essential in industrial environments to prevent unwanted access, bolster data security, and ensure the constant dependability and safety of vital industrial procedures [30, 31].

Recently, several studies have been introduced on the integration of biometric authentication in the Industrial IoT framework. For instance, Das *et al*. [32] presented an improved solution to the growing need for safe and private user-authentication techniques in industrial settings. Another popular work was presented in [33]. The authors investigated biometrics, with particular emphasis on data collection and physiological detection. The health sector is another significant application domain for biometric authentication [34]. Anand *et al*. [35] employed a novel strategy to enhance security for 5G-enabled IoT healthcare systems. They aimed to allay worries about Malware Attack Detection (MAD) and illegal access to private medical data by combining the strength of Convolutional Neural Network (CNN) based techniques with the accuracy of biometric authentication. A method for making a smart health system with biometric authentication was presented in [34]. The goal of this endeavor was to use biometric authentication to enhance healthcare services.

A smart biometric identity-management framework is presented by Farid *et al*. [36] for customized healthcare services. An intelligent multimodal biometric authentication methodology is proposed by Ahamed *et al*. [37] for individualized healthcare services. Another arena for biometric authentication is Cloud and Fog [22–24]. The common goals highlight how important it is to have strong authentication in these decentralized settings. The security issues that arise in cloud systems are discussed in [38, 39], whose authors suggest an automated biometric authentication system that makes use of cloud computing. Other domains include blockchain [23, 39–42], which focuses on cryptographic techniques, decentralized identity, and smart contracts for secure authentication. The emphasis is on bolstering security with creative methods. The biometric technology has shown to be quite useful in the communication sector [23, 41–43]. The importance of the domain is highlighted by the strong emphasis on secure communication. Numerous attempts have been made in the smart IoT sectors [2, 44, 45]. Table IV shows the summary of the publications on the application domains of biometric authentication.

TABLE IV. APPLICATION DOMAINS FOR BIOMETRIC AUTHENTICATION

Domain	Application description	Ref	No of papers
Industrial	Limiting illegal access and preserving the dependability and security of vital industrial processes.	[2, 32, 44–54]	13
Healthcare	Encryption, two-factor authentication, and secure login credentials,	[25–27, 47, 48, 55–57]	8
Cloud	Secured access to cloud services and fog computing nodes.	[22–24, 58–61]	7
Blockchain	Creation of authentication techniques and secure communication protocols.	[23, 39–42]	5
Smart tech	Secure communication and prevent malicious activities	[2, 44, 45, 47, 48, 55–57, 62–64]	11
Communication	Secure communication protocols, encryption, and authentication methods.	[35, 36, 23, 41–43, 58–65]	14
General security	Secure login credentials, two-factor authentication, and encryption.	[2, 33, 34–38, 47–50, 66–104]	51

Fig. 6 illustrates the various application domains of biometric authentication, such as industrial, cloud computing, smart technologies, communication, health care, blockchain, and general security. These applications serve to avert unauthorized accessibility, protect data, and ensure reliability and safety. Additionally, they encompass secure communication protocols and authentications. The figure indicates that “general security” and “communication” are the most prevalent domains for biometric authentication, accounting for 48% and 13% respectively, followed by “industrial” and “smart technology” at 12% and 10% respectively. “Blockchain”, “cloud computing,” and “health” represent 4%, 6%, and 7%, respectively.

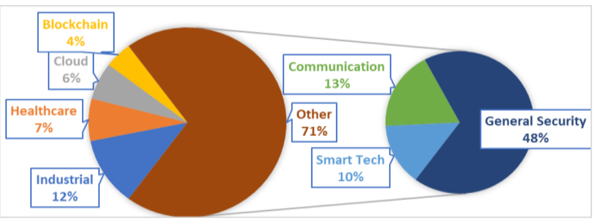

Fig. 6. Application domains of the biometric authentication.

C. RQ2: What Are the Common Deep Learning-Based Biometric Authentication Approaches?

With the advent of AI, a number of approaches have been introduced to solve the biometric authentication problem. This includes face recognition, Iris recognition, and ear recognition. In this section, we address the RQ2 by summarizing the published studies on deep learning-based biometric authentication in the studied papers.

1) Face recognition

The face is perhaps the most commonly used biometric. It serves various purposes, from verifying cellphone users to enhancing security in government buildings and airports through surveillance cameras. Several face recognition-based biometric approaches have been introduced. An enhanced facial recognition approach tailored for IoT applications is proposed by Li *et al*. [105]. Moon *et al*. [106] have introduced a face anti-spoofing technique that employs color segmentation on a field-programmable gate array for face recognition. The matching procedure is carried out on a secure cloud server, while facial features are extracted locally under this distributed architecture. A facial-biometric technique based on DL was presented in [107] for the secure access control of IoT systems. In order to authenticate users, the suggested method uses a CNN for extracting discriminatory facial traits, which are subsequently compared to enrolled templates. Wang and his team proposed the additive margin Softmax objective function in [108] for deep face verification, which is both simple and geometrically interpretable. In 2018, CosFace [109] and ArcFace [110] emerged as two promising face recognition works. AdaCos [111], P2SGrad [112] Uniform Face [113], and Adaptive Face [114] stood out as some of the most promising works.

2) Fingerprint recognition

Fingerprint biometric is one of the most commonly used physiological recognitions techniques, characterized by unique ridge and valley patterns [90]. The application of deep learning for fingerprint recognition has been the subject of numerous studies. For example, Ranjan *et al.* [115] introduced a deep learning method for minutiae extraction that estimates minutiae maps and extracts features at the same time. Similarly, with an emphasis on privacy protection, Yang and associates created a thin fingerprint biometric system for Internet of Things security. The application of generative models to the creation of fingerprint images has also been studied. In order to improve picture connection, a technique based on a generative model was presented in [89] for creating fingerprint images. This algorithm incorporates total variation into the Generative Adversarial Network (GAN) loss function. Furthermore, in order to build a classifier for identifying presentation attacks, the authors created synthetic fingerprints that resembled genuine changed fingerprints in certain ways.

3) Iris recognition

Iris recognition has garnered significant interest in a number of security sectors in recent years. According to Minae *et al*. [116], a remarkably high level of accuracy can be achieved by using features taken from a convolutional neural network that was initially trained on ImageNet. Alaslani and the team's iris recognition system in [117] uses deep features taken from AlexNet for multiclass classification, producing impressive accuracy levels on a variety of datasets. Hofbauer *et al.* [118] presented a CNN-based method for iris image segmentation, showing improved accuracy over earlier techniques. An iris identification system utilizing deep transfer learning was presented in a recent work by Minaee *et al*. [48], which achieved noteworthy accuracy rates on a test dataset by optimizing a pre-trained ResNet model. Minaee and associates [116] came up with a convolutional GAN-powered method for producing realistic-looking artificial iris images. Also, Lee *et al*. [49] presented a GAN-based data augmentation method that produced higher accuracy levels.

4) Palmprint recognition

Recently, palmprints have attracted a lot of interest in the field of biometric identification techniques [52]. A deep-learning framework was used in an early investigation of palmprint identification by Xin *et al*. [119]. Additionally, a study by Samai *et al.* [51] offered a deep-learning technique for 2D and 3D palmprint recognition. An efficient biometric identification system that combines two-dimensional and three-dimensional palmprints at the matching score level was revealed by their research. A Siamese network-based palmprint authorization system was shown by Zhang *et al*. [52]. In order to extract features from two input palmprint photos, two Visual Geometry Group (VGG)-16 networks were used. Izadpanahkakhk *et al*. [53] suggested a transfer learning technique for palmprint verification that simultaneously extracts characteristics and regions of interest from the pictures.

A more recent investigation put forward a sophisticated approach to palmprint authorization by integrating knowledge distillation and hash coding [120]. In Ref. [121], Shao and colleagues demonstrated a transfer convolutional autoencoder-based cross-domain palmprint recognition system. Initially, they utilized convolutional autoencoders for feature extraction in low dimensions. Zhao *et al*. [58] a comprehensive deep feature representation for palm print recognition. The authors designed a CNN architecture for feature extraction from all spectral bands and produced a unified feature.

5) Ear recognition

Ear recognition is a burgeoning field of interest among researchers, with a rising number of biometric recognition investigations centering on ears. Despite not attaining the same level of popularity as facial, iris, and fingerprint recognition, ear recognition is progressively garnering attention. Zhang *et al.* [122] have advocated for the utilization of few-shot learning techniques to facilitate networks in swiftly acquiring the capability to identify images with restricted training data. Sulavko [123] have introduced a distinctive method for generating biometric-based keys and authenticating users by leveraging the acoustic attributes of the outer ear. Dodge *et al.* [124] posited the application of transfer learning in conjunction with deep networks for unconstrained ear recognition.

The impact of ear devices on the recognition process was examined in reference [125], with an emphasis on the possibility of spoofing, especially in a CNN-based framework such as VGG-16. A framework for using CNNs to detect the outer ear image was presented in a paper by Sinha *et al*. [126]. Using discriminant correlation analysis, Omara *et al*. [127] suggested extracting hierarchical deep features from ear pictures and combining them. Last but not least, Hansley *et al*. [128] outperformed other cutting-edge CNN-based techniques for ear detection by combining CNNs with manually created characteristics.

6) Voice recognition

Recently, there has been a surge in interest in delving into deep-learning methodologies for speaker identification. Moreover, a time-delay neural network is presented in [62], which is trained for extracting segments-level "x-vectors" for speech recognition. Researchers propose a technique for deriving speaker embeddings by exploiting joint information. This method involves an encoder-discriminator system similar to that of GAN [63].

7) Signature recognition

There was few research that looked into deep learning's uses in signature recognition prior to its recent rise in prominence. A specialized GAN network was used by Wang *et al.* [80] to introduce signature identification, with the discriminator network's loss value acting as the identification threshold. Tolosana *et al*. [81] suggest an online writers-independent signature authentication technique that leverages Siamese neural network combined with Log Short Term (LSTM) and Gated Recurrent Unit (GRU).

8) Gait recognition

Gait recognition has garnered considerable attention due to its potential uses in areas such as visual surveillance, where a person's gait can be monitored from a distance without active participation [129]. Recently, deep learning techniques for gait recognition have seen increased interest. In one approach, Gait Energy Images (GEIs) are processed using twin CNN networks, where contrastive loss is calculated for minimizing loss for similar inputs and increasing it for dissimilar ones. A time-based LSTM model was used by Battistone *et al*. [130] to present a gait identification technique. This method extracts skeletal data from images and learns joint properties by combining LSTM and dense layers. Similar to this, Zou *et al*. [131] suggested a hybrid DL model that uses information from smartphone sensors, such as the gyroscope and accelerometer, to record gait patterns.

9) ECG signal

Recently, several deep neural networks have been suggested to enhance Electrocardiogram (ECG) analysis tasks. For instance, Hammad *et al.* [132] proposed using CNN as a classifier for ECG biometric authentication. Additionally, in Ref. [133], an enhanced CNN-based biometric system was developed for human authentication, and the method was evaluated using various datasets from Physio Net demonstrating good performance. Zhao *et al.* [134] presented an ECG-based biometric verification scheme that integrates the generalized CNN and S-transformation to improve classification accuracy. The utilization of an enhanced RNN based methods, such as LSTM [56] and GRUs, has significantly enhanced various tasks, including ECG-based biometric recognition. In Ref. [135], a hybrid Restrict Boltmann Machine (RBM) based method integrated with Deep Believe Network (DBN) has been proposed for single-lead ECG classification after detecting ventricular and supraventricular heartbeats. To acquire deep representations for ECG signal classification, GANs can be leveraged to learn without extensive annotated training data [136].

Table V and Table VI shows some important literature on the DL-based biometric authentication and summary of the biometric methods respectively.

TABLE V. SOME IMPORTANT LITERATURE ON THE DL-BASED BIOMETRIC AUTHENTICATION

Ref	Type	Model	Contribution	Results (%)	Disadvantage
[137]	Face	InceptionV3 CNN	Automatic face identification	86.2	Variations in behavioral patterns, acceptance challenges
[138]	Face	CNN	Thermal face recognition	99.65	Data quality, scalability concerns, and computational-resource restrictions
[139]	Face	CNN	Bi-capsule deep face recognition	99.85	Potential challenges in real-time implementation
[140]	Face	AlexNet	Automatic face identification	98.5	Need for diverse datasets
[141]	Face	VGG-16	Automatic face identification	94.4	Limited discussion of implementation Challenges
[113]	Face	RASNet	Face recognition with equidistributed representations	99.8	Potential challenges in real-time implementation on FPGA
[142]	Face	CNN	Multi-view face recognition	99.9	Potential challenges in image quality and data acquisition
[143]	Face	CNN	Multi-view Face recognition	98.52	Complexity of model interpretation
[124]	Voice	AlexNet, VGG16, ResNet50	Ear recognition over small dataset	99.69	Limited analysis of potential false Positives
[144]	Voice	VGG-19, AlexNet, GoogleNet	Domain adaptation on ear recognition	67.53	Data quality, scalability concerns, and computational-resource restrictions
[145]	Voice	AlexNet CNN	Ear recognition with data augmentation	100	Potential challenges in image quality and data acquisition
[146]	Finger	ResNet50	Scalable Fingerprint Recognition	95.7	Complexity
[55]	Finger	CNN	EG-based biometric authentication for military applications	99	Potential challenges in real-time implementation
[56]	ECG	LSTM	ECG identification for personal authentication	88.5	Signal-processing challenges and specialized hardware
[57]	ECG	LSTM	ECG biometric system using hierarchical LSTM	76.8	Complexity of model interpretation
[147]	ECG	LSTM	Automatic Electrocardiogram Sensing Classifier	90.7	Data quality, scalability concerns, and computational-resource restrictions
[148]	ECG	LSTM	detection and localization of myocardial infarction	87.5	Signal-processing challenges and specialized hardware
[84]	Signature	DBN	multimodal biometric system for futuristic security applications	91.5	Limited analysis of potential false Positives
[82]	Signature	DBN	E-Skin for Self-Powered Signature Recognition	99	Complexity
[80]	GAN	DBN	Signature handwriting identification	97	Potential challenges in image quality and data acquisition
[149]	Gait	Capsule network	Multi-view and clothing invariant Gait recognition	74.44	Complexity of model interpretation
[150]	Gait	CNN	Gait recognition with an optimized loss function	100	Potential challenges in real-time implementation on FPGA
[151]	Gait	Pretrained DenseNet	Multi-view Gait recognition	98.87	Complexity of model interpretation
[152]	Gait	CNN	Gait recognition with reduced training time	98.8	Complexity of model interpretation
[153]	Gait	CNN	Gait recognition	86.04	Potential challenges in real-time implementation
[154]	Gait	CNN	Gait recognition with invariance to background motion	99.65	Complexity of model interpretation
[155]	Iris	ResNet and AlexNet	Iris recognition	98.5	Complexity of model interpretation
[156]	Face, Iris	GAN	Super-resolution of diffusion-weighted imaging	79	Limited discussion of implementation Challenges
[157]	Iris	Modified CNN and Soft- max classifier	Iris recognition with improved computational time	96.67	Data quality, scalability concerns, and computational-resource restrictions
[158]	Iris	Inception V2	Noise invariant iris recognition	99.14	Potential challenges in real-time implementation on FPGA

TABLE VI. SUMMARY OF THE BIOMETRIC METHODS

Biometric type	References	No of Papers
Face Recognition	[77, 91, 105–114, 137–143, 159, 160]	23
Fingerprint	[55, 68–75, 88–101, 146]	24
Iris	[2, 47–49, 117, 118, 155–158]	12
Palm Print	[51–54, 58–61, 120, 121]	10
Ear	[122–128]	7
Voice	[62, 63, 124, 144, 145]	4
Signature	[80–84]	7
Gait	[149–154]	5
ECG	[47, 56, 57, 117, 118, 132, 134–136, 147, 148, 161]	15

In Fig. 7, we present the percentage distribution of articles for various biometric authentication methods. The statistic shows that fingerprint recognition is the main topic of evaluated papers (22%). In close succession, 11% of the studies focus on iris recognition and 21% on facial recognition. Moreover, 9% of the articles concentrated on palm print identification, and 14% examined electrocardiograms. Ear and signature recognition methods each account for 7% of the reviewed papers, whereas gait and voice recognition methods represent 5% and 4%, respectively. Table VII compares biometric techniques for practical use cases.

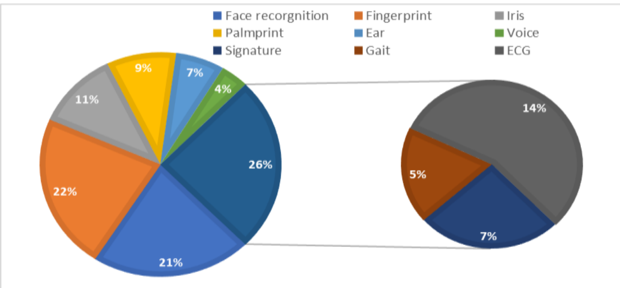

Fig. 7. Distributions of the biometric authentication methods.

TABLE VII. COMPARISONS BETWEEN BIOMETRIC TECHNIQUES, FOR PRACTICAL USE CASES

Biometric Technique	Strengths	Weaknesses	Practical Use Cases
Face Recognition	-Non-intrusive, -High usability	- Sensitive to lighting - Vulnerable to spoofing	- Access control - Surveillance
Fingerprint	- Stable over time -Easy integration	- Requires contact - May fail with dirt	Employee attendance - Physical access
Iris	-High accuracy	- Requires user cooperation	High-security areas
	- Difficult to spoof	- Expensive hardware	Identity verification
Palmprint	- Larger surface area for scanning	-Limited scalability for small devices	Attendance systems
Ear	- Non-intrusive -Unique structure	- Limited use cases	- Forensics - Supplementary biometric systems
Voice	-Non-intrusive - Hands-free operation	- Impacted by background noise	- Call center authentication - Smart assistants
Signature	- Widely accepted - Easy integration	- High intra-user variation - Low accuracy	- Document authentication - E-signatures
Gait	- Non-intrusive - Works at a distance	- Affected by injuries, footwear,	- Surveillance -Continuous authentication
ECG	- Unique physiological trait - Continuous authentication	- Requires contact sensors - Expensive hardware	- Healthcare authentication - Access to medical records

D. What Are the Deep Learning Methods Applied for Biometric Authentication?

Deep Learning (DL) is a subset of ML that leverages representational learning to effectively identify feature representations from raw data [86, 162]. Contrary to classical methods such as random forest and Support Vector Machines (SVM), DL models do not depend on manually crafted features for effective performance. In recent decades, a variety of deep learning approaches have emerged [163], including CNN, RNN, RBM, and GAN. These techniques have been successfully utilized across multiple domains, including computer vision, natural language processing, and medical imaging.

1) Restricted boltzmann machine

For feature learning and network training, the RBM, a generative deep learning technique, uses a greedy, layer-by-layer block structure [135]. To offer objective estimates of maximum likelihood learning, contrastive divergence is used during training [78]. The Deep Belief Network (DBN), a deep learning model created by stacking many Restricted Boltzmann Machines (RBMs), is a well-known illustration of RBM [164]. In order to mimic the distribution between the visible input space and hidden layers, the DBN includes directed connections in the lower levels and undirected connections in the top layer [78]. A layer-by-layer approach is used for training, and contrastive convergence is used to fine-tune the weights.

The complete connections exist between the units in different layers; however, they are not connected within the same layer. "*vi*" denotes the layer that is visible in this context, while "*hi*" denotes the layer that is hidden. Forward and backward directions are not distinguished by RBMs. This indicates that there are equal loads in both directions. RBMs are contrastive divergence algorithm-trained unsupervised learning models. In reference [135], a hybrid RBM-based method integrated with DBN has been proposed for single-lead ECG classification. The proposed method is capable of detecting ventricular and supraventricular heartbeats.

2) Deep belief network

DBN is a type of DL method that utilizes an unsupervised and greedy method [31]. The main objective of designing DBNs is to replicate the human brain in processing complex information and identify intricate patterns. DBN can be conceptualized as a set of RBMs with built-in generative capabilities. DBNs do not have direct connections between nodes within the same network tier. Instead, each node in a DBN is linked to every other node in the layers above and below. In DBNs, the input data depends on the specific type of data being processed [107]. In order to generate an output in a DBN, all layers within the network must incorporate the complete input data. During the training process, every layer uninterruptedly makes ideal selections at each step, which iterates until the desired level of completion for each training process.

DBNs excel at hierarchical feature extraction but require extensive computational resources and are less favored compared to modern architectures like CNNs. They are often used as preprocessing steps for face or voice biometric systems

3) Convolutional neural network

CNN is an interconnected network that has been extensively and widely studied in the realm of DL [88, 165]. This network applies convolution operations to raw data and has found applications in several domains such as image classification, natural language processing, and pattern recognition. The CNN is made up of several layers, including convolutional layers and pooling layers, all of which are stacked together to enable autonomous feature extraction within a deep architecture. During training, the model minimizes a loss function, such as cross-entropy, using optimization algorithms like Adam. Regularization techniques like dropout and data augmentation are employed to reduce overfitting. After training, the model is evaluated. Recently, several CNN modes have been proposed in various studies, which include AlexNet [166], VGG [167], and GoogleNet [168]. In order to authenticate users, some authors used CNN for extracting discriminatory facial traits, which are subsequently compared to enrolled templates. Wang and his team proposed the additive margin SoftMax objective function in reference [108] for deep face verification. The proposed model is both simple and geometrically interpretable. In order to extract features from two input palmprint photos, two VGG-16 networks were used. The authors of another work in reference [53] suggested a transfer learning technique for palmprint verification that simultaneously extracts characteristics and regions of interest from the pictures.

4) Recurrent neural networks

RNNs use the hidden unit of the recurrent cell to capture sequential input over time, enabling the network to learn complex patterns [57]. The network's information is continuously updated to reflect the current state, with the hidden unit cells being adaptable. However, RNNs face challenges in modeling long-term activity sequences and temporal dependencies due to training difficulties and issues with vanishing or bursting gradients. To address these challenges, variations of RNNs such as the Gated Recurrent Unit (GRU) and Long Short Term Memory (LSTM) have been introduced [56]. In order to regulate the influx of input into the network, LSTM incorporated a memory cell for storing contextual data [81]. This enables the model to effectively capture global features, improving performance and modeling temporal dependencies in sequential data [56]. However, a major drawback of LSTM is the high number of parameters that require adjustment during training. To address this issue, the GRU was introduced as a faster and simpler alternative with fewer parameters that need updating. The method of updating the next hidden state and the technique for revealing contents differ between GRU and LSTM. While LSTM uses a summing operation, GRU updates the next hidden state based on correlation, taking into account the time needed to retain information in memory.

A time-based LSTM model was used by Battistone *et al*. [130] to present a gait identification technique. This method extracts skeletal data from images and learns joint properties by combining LSTM and dense layers. The utilization of enhanced RNN-based methods, such as LSTM [56] and GRUs, has significantly enhanced various tasks, including ECG-based biometric recognition.

Implementation begins with preprocessing input sequences into fixed-length segments. The RNN, often enhanced with LSTM or GRU, processes each sequence step-by-step, updating its hidden state. Backpropagation Through Time (BPTT) is used to minimize the loss over all time steps. Regularization techniques, such as gradient clipping, prevent exploding gradients

5) Auto-Encoder

Auto-encoders are used to learn effective data encoding in an unsupervised way [121]. This is accomplished by first compressing the input data into a latent-space representation, from which the output, which is often identical to the input, is then rebuilt. The Autoencoder (AE) method utilizes encoder and decoder units to replicate input values as output [79]. Autoencoder techniques extract important features from unlabeled data by using a reduced-dimensional space projection. To reduce errors, the encoder converts input data into hidden features, which the decoder subsequently reconstructs. The approach promotes data-driven learning feature extraction approaches to avoid problems with manually produced features. By making sure that the hidden units are smaller than the inputs or outputs, the autoencoder is trained to generate a lower-dimensional discriminative feature [79]. The model training involves minimizing reconstruction loss, such as Mean Squared Error (MSE). AEs are useful in anomaly detection by measuring reconstruction errors, with higher errors indicating deviations. Advanced variations, such as denoising autoencoders, add noise to the input to improve robustness.

Various variations of autoencoders have been proposed in the past. One of the most popular is the Stacked Denoising Auto-Encoders (SDAEs), which stack numerous AE and uses them for picture denoising [121]. Another popular autoencoder variation that makes use of a prior distribution on the latent representation is the Variational Auto-Encoder (VAE). VAEs are powerful tools for generating synthetic biometric data, enabling systems to generalize across varying demographics, lighting fixtures, and environmental conditions. Their ability to create diverse, privacy-preserving datasets is invaluable in training robust and unbiased biometric models.

6) Generative adversarial network

In Ref. [169], the Generative Adversarial Network (GAN) concept was first presented. An alternate method to the conventional maximum likelihood estimation process is offered by GAN. It uses both unsupervised and unsupervised processes in a game-like interaction between two network models. Training a generative model that can precisely estimate the spreading of the target data using the given training data is the main goal of GAN [90]. Furthermore, GAN integrates a discriminative model that evaluates whether a sample data set comes from the produced output or the real training data. The learning rate and the model structure are two of the many variables that affect the GAN training process [89].

To ensure effective convergence, several ad hoc tactics are often employed to enhance the reliability of the generated data. Several GAN method extensions have been developed to enhance convergence and simplify the training phase [170]. However, research on GAN is still in its nascent stages. Recent studies have indicated that supervised learning can be combined with GAN, offering potential benefits for information retrieval and recommender systems [120].

GANs play a transformative role in generating artificial biometric data, enabling systems to generalize across diverse demographics, lighting conditions, and environments [90]. By addressing data scarcity and variability, GANs significantly enhance the robustness, fairness, and accuracy of biometric systems. However, ensuring ethical usage and addressing technical challenges remain critical for their broader adoption in real-world applications. GANs consist of two neural networks, a generator and a discriminator trained in an adversarial setup. The generator creates synthetic biometric data while the discriminator distinguishes between real and synthetic data. Training involves alternating updates to minimize the generator's loss and maximize the discriminator's ability to detect fakes. Techniques like Wasserstein loss or spectral normalization improve convergence stability.

Several works have been introduced to exploit GAN for biometric authentication for example To improve picture connection, a technique based on a generative model was presented in Ref. [89] for creating fingerprint images. This algorithm incorporates total variation into the GAN loss function. Furthermore, in order to build a classifier for identifying presentation attacks, the authors created synthetic fingerprints that resembled genuine changed fingerprints in certain ways.

TABLE VIII. DEEP LEARNING METHODS FOR THE BIOMETRIC AUTHENTICATION

Model	References	No of papers
CNN	[35, 50–53, 58–60, 68–70, 75, 77, 88, 91, 93–101, 106, 107, 122–128, 132, 134, 147, 148, 159, 161, 171–174]	42
DNN	[64, 85, 86, 175]	4
DBN	[62, 65, 84, 87, 107]	5
RNN	[56, 57, 72, 73, 81, 107, 130, 131, 176]	9
RBM	[78, 84, 135, 164]	4
AE	[79, 121, 176–178]	5
GAN	[49, 54, 60, 61, 63, 74–76, 80, 89, 90, 120, 136, 156]	14

Table VIII and Fig. 8 illustrate the distribution of papers that employed deep learning algorithms for the biometric authentication methods identified in the Systematic Literature Review (SLR). From the figure, it is evident that the majority of the articles selected for the SLR utilize CNNs, which are featured in 51% of the studies. GANs and RNNs are used in 16% and 11% of the papers, respectively. Deep Belief Networks (DBNs) and Autoencoders (AEs) each appear in 6% of the articles. Finally, deep neural networks (DNNs) and RBMs are represented in 5% of the total reviewed articles for the SLR.

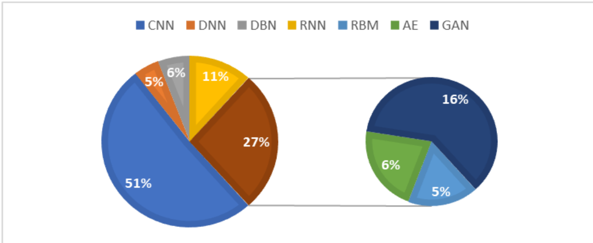

Fig. 8. Distribution of the deep learning-based techniques.

E. *RQ4: What are Popular Evaluation Metrics Used for the Deep Learning Base Biometric Authentication Method?*

Although no standardized evaluation metrics are exclusively used for assessing machine learning techniques in biometric authentication, various performance measures have been applied by different researchers. These include the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER), along with other metrics such as accuracy (acc), recall (rec), precision (pre), F1, False Negative Rate (FNR), and specificity. The performance metrics employed in the reviewed studies based on the selected articles are presented in this section.

The FAR [35, 172] represents the likelihood of mistakenly identifying samples from different individuals as belonging to the same individual. In the context of ML-based authentication techniques, the classification threshold preference can lead to incorrect recognition of deceivers' characteristics. FRR [35, 172] represents the likelihood of mistakenly identifying samples from the same individual as belonging to different individuals. The EER [106, 179] is the point where the FAR and FRR are equal. As FAR and FRR are inversely related, an increase in one leads to a decrease in the other. In biometric applications, understanding the trade-offs between FAR, FRR, and EER is crucial for optimizing system performance [106]. FAR refers to the probability that a biometric system incorrectly accepts an unauthorized user, while FRR represents the likelihood of rejecting a legitimate user. In high-security settings, a low FAR is essential to prevent unauthorized access, but this often comes at the cost of a higher FRR, where legitimate users may be incorrectly denied access. The EER, the point at which FAR and FRR are equal, serves as a useful benchmark for system balance [179]. In applications demanding excessive protection, minimizing FAR is often prioritized, which may lead to increased FRR and potential user frustration.

While precision measures the accuracy of positive forecasts, accuracy measures the total number of accurate predictions. Recall, also known as sensitivity, is the percentage of positive cases that the classifier properly detects. The two values have an adverse connection, even though one may want to maximize both precision and recall. A decrease in recall could result from increasing precision, and vice versa. We term this phenomenon the precision/recall trade-off. The F-score, which is the harmonic mean of precision and recall, is a more useful metric to take into account than maximizing recall and precision separately. By adjusting the decision threshold for a classifier, one can observe changes in performance in terms of the trade-off between recall and precision.

Table IX and Fig. 9 displays the performance measure formulas and the corresponding number of papers for each metric. Models with lower performance measure values demonstrate a higher capacity for generalization when it comes to FPR and FNR. The table also makes it clear that the symbols True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) stand for true positive, false positive, and false negative, respectively.

TABLE IX. PERFORMANCE EVALUATION METRICS

Metrics	Formula	References	No of Papers
Accuracy	$\frac{TN+TP}{(TN+FN+FP+TP)}$	[2, 25–27, 35, 36, 47, 51–53, 56, 58, 59, 66, 77–79, 81, 91–93, 106–112, 114, 122–128, 130, 131, 144, 146–148, 159, 160, 164, 171–174, 180–185]	55
Recall/ Sensibility	$\frac{TP}{(TP+FN)}$	[35, 58, 59, 75, 77, 91, 93–100, 106, 107, 122, 123, 127, 124, 128, 147, 148, 159, 171–174]	28
Precision	$\frac{TP}{(TP+FP)}$	[27, 35, 47, 50, 60, 68–70, 75, 77, 91, 93–100, 106, 107, 123, 127, 128, 159, 172–174]	28
FRR	$\frac{FN}{TP+FN}\times 100$	[2, 25–27, 35, 47, 53, 58, 66, 172]	10
FAR	$\frac{FP}{FP+TN}\times 100$	[2, 35, 53, 58, 77, 79, 93, 122, 126, 127, 172]	11
EER	-	[63, 80, 106, 186–192]	10

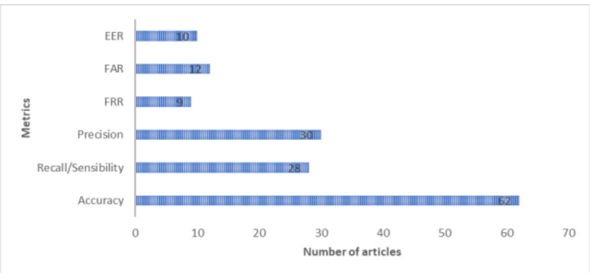

Fig. 9. Summary of the evaluation metrics.

Overfitting is a common challenge in deep learning, particularly in biometric systems, where models learn excessively from training data, failing to generalize to unseen data [88, 165]. Biometric systems often deal with sensitive data like fingerprints, facial recognition, and ECG signals, making the need for robust optimization strategies critical. Table X shows key optimization strategies to mitigate overfitting, with emphasis on their importance in biometric models:

TABLE X. KEY OPTIMIZATION STRATEGIES TO MITIGATE THE OVERFTTING

Optimization Strategy	How it Works	Advantages	Application in Biometric Models
Batch Normalization	Normalizes layer inputs by adjusting and scaling activations within each mini-batch.	Accelerates training.	Handles variability in biometric data like facial images or ECG signals. [147, 148]
		Reduces internal covariate shift	Improves generalization across diverse datasets [165]
		Allows higher learning rates.	Stabilizes training for complex architectures. [134]
Dropout	Randomly disables a fraction of neurons during training.	Prevents over-reliance on specific neurons.	Mitigates overfitting in small biometric datasets. [134]
			Forces models to learn redundant, generalizable representations. [68, 101]
		Reduces dependency on large datasets.	Simulates real-world variations (e.g., different lighting, noise, or occlusions). [132, 161]
L2 Regularization	Adds a penalty term to the loss function proportional to the sum of squared weights.	Discourages large weights.	Promotes simplicity in biometric models to improve interpretability. [49, 60]
		Simplifies the model.	Ensures stability in learning subtle patterns (e.g., facial landmarks or fingerprint details)
Early Stopping	Monitors validation loss and halts training when performance degrades.	Prevents overtraining.	Ensures models generalize well to unseen biometric data [132, 161].
		Improves feature learning.	Enhances adaptability to unique biometric features like iris patterns or ECG signals.

F. *RQ 5: What are the Research Challenges in Biometric Authentication?*

This section focuses on addressing RQ4 by exploring the research challenges associated with deep learning-based biometric authentication. Despite significant advancements and contributions in this domain, several critical challenges persist. These unresolved issues not only highlight the limitations of current methodologies but also pave the way for future research and innovation in the field. The key challenges include datasets, biometrics, interpretability, complexity and scalability, privacy and access control, and adversarial attacks. Details of the challenges are outlined below:

1) Datasets issue

DL has demonstrated significant promise and effectiveness in the fields of computer vision and pattern recognition, including biometric authentication. Yet, the majority of datasets that are currently accessible for deep learning applications in biometric research are terribly unbalanced [49, 60, 77, 88, 91, 105–107, 109, 132, 159, 161, 185, 193]. Biometric recognition may be skewed as a result of a training dataset imbalance. To overcome imaging and sophisticated annotation restrictions, future work should concentrate on creating extensive public databases and private datasets. Oversampling strategies have been used in several studies to address the issue of imbalanced data [194].

To address dataset imbalance in biometric data, techniques like Synthetic Minority Oversampling Technique (SMOTE) and Adaptive Synthetic Sampling (ADASYN) can be effective but must be applied carefully to preserve data integrity [195]. SMOTE generates synthetic samples by interpolating minority class data, but in biometric records, this can introduce unrealistic patterns that may affect accuracy. ADASYN, which focuses on creating synthetic samples for more complex, hard-to-classify data points, can sometimes amplify noise or create ambiguous patterns. Moreover, in dealing with imbalanced biometric datasets, the precision-recall trade-off is crucial. Precision measures the proportion of correctly identified positive cases (e.g., legitimate users) out of all cases flagged as positive by the model, while Recall measures the proportion of actual positive cases correctly identified by the model. When datasets are imbalanced, where one class vastly outnumbers the other, increasing precision often leads to a decrease in recall and vice versa. Future research should examine other oversampling and under sampling techniques, as studies have shown that these methods may induce biases dependent on sample selection [196].

2) Biometric fusion

Single biometric recognition alone is not enough to address all the deep learning-based biometric tasks [132, 197]. For instance, it may not be feasible to differentiate between identical twins based solely on their faces or to match an identity when the face is disguised or altered through surgery. However, by combining information from various biometrics, a more consistent solution can be achieved [37]. For example, using a combination of voice and face or voice and gait can potentially solve the problem of identifying identical twins [132]. However, developing a DL-based method that can effectively encode and aggregate different biometrics would be an intriguing challenge. Information fusion can occur at various levels, such as the data level, feature level, score level, or decision level [197]. Although there have been several studies on biometric fusion [5, 37, 132, 198], most of them are still in their early stages and do not yet encompass the real-world scale of biometric recognition.

To strengthen multi-modal biometric systems, unique methodologies for feature-level fusion and score-level fusion can be employed to effectively combine information from different biometric modalities, enhancing the accuracy and robustness of the system. For feature-level fusion, one effective approach is Canonical Correlation Analysis, which seeks to find the linear relationship between two sets of features from different modalities, maximizing the correlation between them. In score-level fusion, where the outputs from individual classifiers are combined, min-max normalization is a widely used method.

Hybrid models combining CNN and RNN are ideal for temporal biometric data like gait or voice. The CNN extracts spatial features from input sequences (e.g., spectrograms or frames), while the RNN processes temporal dependencies, capturing sequential patterns. Ensemble techniques, integrating multiple such hybrid models, further enhance accuracy and robustness by leveraging complementary strengths across diverse architectures.

3) Interpretable deep architecture

DL-based methods have undeniably proved outstanding performance in various scenarios, including partial data and different sensor types [199]. However, challenges persist in these areas [9, 48, 198]. Furthermore, in real-world scenarios, the number of subjects or people should ideally reach tens of millions. Consequently, biometrics datasets need to encompass a significantly larger number of classes, ranging from 10 million to 100 million [193]. These datasets also need to incorporate challenging benchmarks. Despite these advancements, there are still several unanswered questions regarding deep learning models [55, 67, 187]. For instance, what exactly do these models learn? Why are they susceptible to being deceived by adversarial examples, whereas humans can easily detect them? Additionally, what is the minimal neural architecture capable of achieving a certain level of recognition accuracy on a given dataset? Post-hoc interpretability strategies like LIME (Local Interpretable Model-Agnostic Explanations) and SHAP (SHapley Additive exPlanations) help explain predictions in biometric systems by analyzing feature contributions after the model has made decisions.

4) Complexity and scalability

Deep learning model training for biometric identification is a resource-intensive process that calls for a large amount of memory, storage, and processing power [77, 106]. This may be a problem for businesses with little funding. Furthermore, putting in place real-time biometric authentication systems necessitates that the model make judgments quickly and with little delay. It can be difficult to do this technically while keeping security and accuracy intact. Several studies highlight the importance of complexity and scalability as the main issues for researchers in [48, 77, 88, 91, 105–110, 132, 159, 161]. It is vital to make sure that authentication systems can sustain dependability and scale efficiently as IoT networks grow. The issues presented by the growing scale and complexity of biometric ecosystems are thus the focus of future attention.

Quantization and pruning are essential techniques for reducing the model size and enhancing memory efficiency in edge devices, which often have limited computational and storage resources [132]. Quantization involves converting model weights and activations from high-precision to lower precision, significantly reducing the model's memory footprint and computational demands while maintaining acceptable accuracy. Pruning, on the other hand, removes redundant or less important parameters, such as zeroing out small weights or entire neurons in the network, resulting in a sparser model that requires fewer storage and computation resources [132, 161].

5) Privacy and access control

Biometric data is inherently sensitive, and its misuse or unauthorized access can lead to severe privacy violations. Deep learning models require this data for training, raising concerns about data security and the potential for data breaches. Furthermore, the use of biometric data, particularly in surveillance applications, raises ethical questions regarding consent, data ownership, and the potential for misuse by governments or corporations. Thus, Privacy concerns have been highlighted in various studies as crucial issues [2, 6, 33, 107]. Researchers are working towards developing authentication systems that prioritize user privacy and provide efficient access management.

6) Adversarial attacks

Deep learning models, which can be used in biometric authentication, for instance, can be subjected to adversarial attacks [89, 90]. Different from traditional machine learning algorithms, the attackers can deceive models into misjudging the identity of a person and acquire unauthorized access via even altering some input data perturbation (e.g., a face image). However, deep learning can also be deceived by fakes: fake fingerprints or a photograph with high image sharpness. Amidst these, there is still a big challenge in developing credible biometric authentication systems; hence [63, 80, 120, 136, 156].

Table XI and Fig. 10 list the major research projects that have tackled the difficulties associated with DL-based biometric authentication. A thorough examination of this research shows that, of the different difficulties noted, complexity and scalability stand out as the most important and often cited problems. More emphasis is placed on these issues in the literature, demonstrating their significant influence on the creation and application of reliable biometric authentication techniques. The importance of complexity and scalability indicates that these issues are crucial for practitioners and researchers who want to improve the dependability and efficiency of biometric systems in practical settings.

TABLE XI. CHALLENGES OF THE DEEP LEARNING BASED BIOMETRIC AUTHENTICATION

Challenges	References	No of papers
Datasets Issue	[9, 33, 49, 51–53, 56, 60, 77, 88, 91, 105–107, 109, 123, 132, 134, 159, 161, 185, 193]	22
Biometric Fusion	[5, 37, 49, 50, 55, 83, 84, 58, 67, 132, 187, 193, 197, 198]	14
Interpretable Deep Architecture	[9, 48, 85, 86, 175, 198]	6
Complexity and Scalability	[2, 48, 49, 58, 59, 77, 88, 91, 105–110, 122, 132, 135, 147, 148, 159, 161, 165, 171, 193, 200]	25
Privacy and Access Control	[2, 6, 23, 32, 33, 38, 66–71, 102, 107, 193]	15
Adversarial Atack	[49, 54, 63, 80, 89, 90, 120, 136]	8

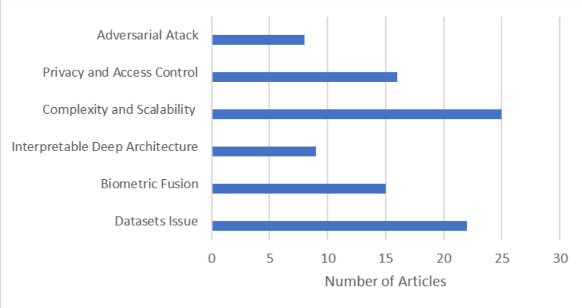

Fig. 10. The challenges of biometric authentication.

G. What are the Future Trends to Address the Challenges in Deep Learning-Based Biometric Authentication?

It is also important to articulate those future directions in the authentication research. These paths correspond to the goals that researchers should meet so they can advance in this domain, overcome new challenges, and extend the interoperability of authentication protocols. Future directions provide researchers with signposts to real objectives that could help strengthen the security, effectiveness, and applicability of what we do during practice time, as well as new technologies.

1) Synthetic data generation and augmentation

By simulating the real world in a virtual environment, one can generate an enhanced version of biometric data to enhance model performance along with boosting its generalization properties. For example, techniques like GANs [49, 54, 63, 80, 89, 90, 120, 136, 156] can generate high-quality realistic biometric data using which it is possible to train a state-of-the-art deep learning model without the need for extensive quantities of real-world/real-scenario training data. Advanced data augmentation techniques, such as multi-modal augmentation, can help improve model robustness by simulating a wide range of conditions, such as variations in lighting, pose, and facial expressions [80, 136]. This leads to better generalization across different environments and populations.

2) Security robustness and enhancement

Adversarial training is one of the major tools to improve robustness in deep learning models, which helps security vulnerabilities such as adversarial attacks [49, 54, 120], otherwise. This means training models on clean data while also making them robust to attacks from adversaries spoofing inputs. Flexible and general-purpose purpose-software architectures are currently under research to improve the security resilience [2, 33, 38, 66–71, 103, 132, 135, 201] while other architecture trends focus on significantly increasing resource sharing as a result of advances in node efficiency (see Sect. Optimization techniques to extract features and ensemble methods that add outputs from multiple models can avoid the attack.

Antagonistic training techniques, such as the Fast Gradient Sign Method (FGSM) and Projected Gradient Descent (PGD), are increasingly used to enhance the robustness of biometric models against spoofing and input perturbations [71, 132, 135]. These techniques involve deliberately crafting adversarial examples, which are inputs modified with small but strategically designed perturbations to mislead the model into making incorrect predictions. FGSM works by calculating the gradient of the model's loss function with respect to the input data. On the other hand, PGD performs a more refined process, iteratively perturbing the input and projecting it back into a feasible space.

Adaptive multi-modal fusion approaches can be highly effective [58, 59]. This strategy integrates multiple biometric modalities such as face, fingerprint, and voice into a unified system, where each modality provides complementary information. The adaptive fusion allows the system to dynamically weigh the importance of each modality based on the quality and reliability of the data, adjusting for potential perturbations or spoofing attempts that may affect one modality more than others may [24].

3) Real-time authentication

The growing threat of cyber-attacks, distant identification thefts, session hijacking, or unauthorized entries on devices such as smartphones and databases has potential limitations in using traditional authentication mechanisms [6, 8, 94–97] which read time-critical scenarios like unlocking a phone to authenticate as a password keeper or to authorize an e-payment. Real-time authentication utilizes state-of-the-art technologies, and deep learning plays a crucial part in examining various biometric & behavioral properties. This method improves security but also makes the user experience more pleasant by not always requiring repetitive authorization alerts [94, 95].

Zero-Knowledge Proofs (ZKPs) offer a powerful solution for secure authentication without revealing sensitive biometric data, thus enhancing user privacy. In a ZKP framework, a user can prove they possess valid biometric credentials without actually disclosing the biometric data itself. The core principle of ZKPs is that the prover can convince the verifier of the truth of a statement [95, 96].

4) Shot and self-supervised learning

Many successful approaches, especially those introduced for biometric recognition, have learned their model on the basis of large datasets with enough number of samples per class [85, 86, 79]. An exciting prospect in this domain that will emerge soon is the growing popularity of powerful methods from just a few shots or even one shot in extreme cases [3]. This development would let create discriminative models without the requirement for generating substantial numbers of samples from every specific ID. A emerging topic in deep learning is self-supervised learning [13, 202], however it has not been fully explored either on biometric recognition. The reason is that we have not applied to the region of patches with a smaller size, where it could serve as an area for the network to learn discriminative biometric features and then pool them together in order to verify if this image corresponds or not (classification task) [200].

5) Blockchain integration

Eliminating central points of control or failure is one of the main advantages of combining blockchain technology with biometric authentication [30]. Conventional solutions frequently use centralized servers for device management and authentication, which leaves holes that hackers could take advantage of. Another essential component of blockchain that improves authentication is its immutability [39]. Once information is recorded on a blockchain, it cannot be removed or changed without the network's approval. In IoT contexts, where data integrity is crucial, this feature is especially beneficial. Blockchain guarantees that all activities inside the Internet of Things network are traceable and impenetrable by logging device interactions, authentication events, and data exchanges on an unchangeable ledger. Many studies have focused on identifying the possibilities of blockchain technology in authentication systems, as mentioned in Refs. [23, 24, 30, 39, 40].

Blockchain-based decentralized data storage leverages a distributed network of nodes to store data across multiple locations, ensuring enhanced security and integrity [23, 40]. Unlike traditional centralized systems, where data is stored in a single location, blockchain stores data in blocks that are cryptographically linked together in a chain. Each block contains a batch of transactions or data entries, along with a cryptographic hash of the previous block, creating an immutable record [23]. This hashing ensures that once data is written to the blockchain, it cannot be altered without changing all subsequent blocks, making tampering virtually impossible.

6) IoT and wearable technology integration

From industrial automation and personal security to smart homes and health monitoring, wearable technology and the Internet of Things are transforming many facets of our everyday lives [66]. Biometric authentication systems are increasingly integrating various technologies as they develop [2, 33, 34, 38, 22–24, 58, 59, 66–70] As a result of this integration, more secure, smooth, and customized authentication techniques that work in real-time across a variety of devices and situations are being developed. Biometric authentication may be integrated with wearables and the Internet of Things to develop continuous, context-aware, and highly secure authentication systems that protect sensitive data and improve user comfort [68]. This integration is especially important in situations like mobile and distant locations when conventional authentication techniques are inadequate or unfeasible [66–68].

Hierarchical deployment strategies for real-time biometric data processing combine the strengths of cloud and edge computing to achieve efficient and secure operations [24, 58]. At the edge level, biometric data is captured and preprocessed locally on edge devices, such as IoT sensors or edge servers, ensuring low latency and reducing the volume of data transmitted to the cloud. Critical tasks like feature extraction, encryption, and initial authentication can occur here to enhance responsiveness and data protection [58, 59].

Table XII and Fig. 11 present a visual depiction of the anticipated future trends designed to tackle the challenges faced in deep learning-based biometric authentication, as outlined in multiple studies. The figure illustrates that multiple emerging trends have been identified in the literature to tackle the diverse challenges associated with biometric authentication. Notably, among these trends, the integration of IoT devices and wearable technology stands out as the most promising and widely discussed future direction. This trend is emphasized in the literature as having significant potential for enhancing the effectiveness, security, and usability of biometric systems, offering innovative solutions to overcome the current limitations in the field.

TABLE XII. THE FUTURE TRENDS OF DEEP LEARNING-BASED BIOMETRIC AUTHENTICATION

Future trends	References	No of papers
Synthetic Data Generation and Augmentation	[49, 54, 63, 80, 89, 90, 120, 136, 156]	9
Robustness and Enhancement	[2, 33, 38, 58, 59, 66–71, 103, 122, 132, 135, 147, 148, 171, 201]	18
Realtime Authentication	[6, 8, 94–97, 103, 132, 135, 165, 193, 200]	12
Self-Supervised Learning	[3, 9, 13, 53, 79, 85, 86, 175, 182, 200, 202]	11
IoT and Wearable Technology Integration	[2, 5, 22–25, 30, 33–39, 43, 58–62, 66–71, 107]	27
Blockchain Integration	[23, 24, 30, 39–42]	7

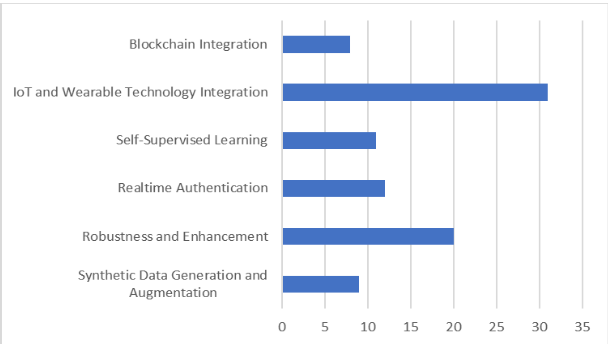

Fig. 11. The future trends to address the challenges.

V. CONCLUSION

The integration of machine learning has greatly improved biometric systems, especially in the realm of deep learning techniques. With the continuous expansion of modern technology, there are both security challenges and opportunities for biometrics to be utilized in various applications. In this study, we performed an SLR to thoroughly explore and summarize the current research on deep learning-based biometric authentication techniques. The review adhered to the PRISMA methodology, employing established protocols to gather, synthesize, and present relevant articles. We applied targeted search strategies across major electronic databases, ultimately selecting and analyzing 109 articles for inclusion in the SLR. The review identified and summarized the popular biometric techniques used for authentication, the common deep learning methods applied in biometric authentication, and the widely used evaluation metrics for deep learning-based biometric authentication. Additionally, the paper highlighted the main challenges in deep learning-based biometric authentication and discussed future trends in the field.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

AA and NHK conducted the research; SNHSA mainly analyzed the data; AA and NHK wrote the paper; all authors had approved the final version.

REFERENCES

[1] B. C. Arjun and H. N. Prakash, "Multimodal biometric recognition system using face and finger vein biometric traits with feature and decision level fusion techniques," *Int. J. Comput. Theory Eng.*, vol. 13, no. 4, pp. 123–128, 2021.

[2] C. Annadurai, I. Nelson, K. N. Devi, R. Manikandan, N. Z. Jhanjhi, M. Masud, and A. Sheikh, "Biometric authentication-based intrusion detection using artificial intelligence internet of things in smart city," *Energies*, 2022. doi: 10.3390/en15197430

[3] K. Sundararajan and D. L. Woodard, "Deep learning for biometrics: A survey," *ACM Comput. Surv*, vol. 51, no. 3, pp. 1–34, 2018. doi: 10.1145/3190618

[4] K. Shaheed, A. Mao, I. Qureshi, M. Kumar, Q. Abbas, I. Ullah, and X. Zhang, "A systematic review on physiological-based biometric recognition systems: current and future trends," *Arch. Comput. Methods Eng*, pp. 1–44, 2021.

[5] A. Wells and A. B. Usman, "Trust and Voice Biometrics Authentication for Internet of Things," *International Journal of Information Security and Privacy*, vol. 17, no. 1, pp. 1–28, 2023.

[6] N. H. Kamarudin, J. J. Siong, M. I. Solihin, and G. Hayder, *Multilevel Authentication in Smart Online Classroom Attendance BT - Sustainability Challenges and Delivering Practical Engineering Solutions*, G. H. A. Salih and R. A. Saeed, Eds., Cham: Springer International Publishing, 2023, pp. 171–176.

[7] Q. Xue, X. Ju, H. Zhu, H. Zhu, F. Li, and X. Zheng, "A biometric-based IoT device identity authentication scheme," in *Proc. First EAI International Conference on Artificial Intelligence for Communications and Networks, AICON 2019, Harbin, China, May 25–26, 2019, Proceedings, Part II 1*, Springer, 2019, pp. 139–149.

[8] M. Y. S. Krishna, A. Arya, S. Ansari, S. Awasya, J. Sushakar, and N. Uikey, "Real time door unlocking system using facial biometrics based on IoT and Python," in *Proc. 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, 2023, pp. 1–5. doi: 10.1109/SCEECS57921.2023.10063142

[9] C. Lau, H. Leong, J. Chuah, and N. H. Kamarudin, "An eye fatigue recognition system using YOLOv2," in *Proc. 2021 Innovations in Power and Advanced Computing Technologies (i-PACT)*, IEEE, 2021.

[10] S. Yang and B. Chen, "Effective surrogate gradient learning with high-order information bottleneck for spike-based machine intelligence," *IEEE Trans. Neural Networks Learn. Syst.*, pp. 1–15, 2023. doi: 10.1109/TNNLS.2023.3329525

[11] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for internet-of-things security: A review," *Sensors*, vol. 21, no. 18, 6163, 2021.

[12] I. Tomičić, P. Grd, and M. Bača, "A review of soft biometrics for IoT," in *Proc. 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, IEEE, 2018, pp. 1115–1120.

[13] M. Gayathri, C. Malathy, and M. Prabhakaran, "A review on various biometric techniques, its features, methods, security issues and application areas," in *Proc. 2019 Internation Conference on Comput. Vis. Bio-Inspired Comput. ICCVBIC 2019*, 2020, pp. 931–941.

[14] S. B. Junaid, A. A. Imam, A. N. Shuaibu, S. Basri, G. Kumar, Y.A. Surakat, A. O. Balogun, M. Abdulkarim, A. Garba, Y. Sahalu, A. Mohammed, Y. T. Mohammed, B. A. Abdulkadir, A. A. Abba, N. A. I. Kakumi, and A. K. Alazzawi, "Artificial intelligence, sensors and vital health signs: a review," *Appl. Sci.*, vol. 12, no. 22, 11475, 2022.

[15] A. Z. Khoirunnisaa, L. Hakim, and A. D. Wibawa, "The biometrics system based on iris image processing: A review," in *Proc. 2019 2nd International Conference of Computer and Informatics Engineering (IC2IE)*, IEEE, 2019, pp. 164–169.

[16] S. C. Mukhopadhyay, S. K. S. Tyagi, N. K. Suryadevara, V. Piuri, F. Scotti, and S. Zeadally, "Artificial intelligence-based sensors for next generation IoT applications: A review," *IEEE Sens. J.*, vol. 21, no. 22, pp. 24920–24932, 2021.

[17] A. Ross, S. Banerjee, and A. Chowdhury, "Security in smart cities: A brief review of digital forensic schemes for biometric data," *Pattern Recognit. Lett.*, vol. 138, pp. 346–354, 2020.

[18] R. Karthick, R. Ramkumar, M. Akram, and M. V. Kumar, "Overcome the challenges in bio-medical instruments using IOT–A review," *Mater. Today Proc.*, vol. 45, pp. 1614–1619, 2021.

[19] M. M. Mariani, R. Perez-Vega, and J. Wirtz, "AI in marketing, consumer research and psychology: A systematic literature review and research agenda," *Psychol. Mark.*, vol. 39, no. 4, pp. 755–776, 2022.

[20] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 9128–9143, 2020.

[21] M. J. Page, J. E. McKenzie *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, 2021. doi: 10.1136/bmj.n71

[22] M. H. M. Saad, M. H. S. Akmar, A. S. S. Ahmad, K. Habib, A. Hussain, and A. Ayob, "Design, development & evaluation of a lightweight IoT platform for engineering & scientific applications," in *Proc. 2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*, IEEE, 2021, pp. 271–276.

[23] B. Singh, R. Lal, and S. Singla, "A secure Authentication mechanism for accessing IoT devices through mobile App," in *Proc. 2022 International Conference on Computational Modelling, Simulation and Optimization (ICCMSO)*, IEEE, 2022, pp. 274–278.

[24] A. Rana, A. S. Rawat, A. Afifi, R. Singh, M. Rashid, A. Gehlot, S. V. Akram, and S. S. Alshamrani, "A long-range internet of things-based advanced vehicle pollution monitoring system with node authentication and blockchain," *Appl. Sci.*, vol. 12, no. 15, 7547, 2022.

[25] N. El-Meniawy, M. R. M. Rizk, M. A. Ahmed, and M. Saleh, "An authentication protocol for the medical internet of things," *Symmetry (Basel).*, vol. 14, no. 7, 1483, 2022.

[26] J. Liu, J. Yang, W. Wu, X. Huang, and Y. Xiang, "Lightweight authentication scheme for data dissemination in cloud-assisted healthcare IoT," *IEEE Trans. Comput.*, vol. 72, no. 5, pp. 1384–1395, 2022.

[27] A. Mehbodniya, J. L. Webber, R. Neware, F. Arslan, R. V. Pamba, and M. Shabaz, "Modified lamport merkle digital signature blockchain framework for authentication of internet of things healthcare data," *Expert Syst.*, vol. 39, no. 10, e12978, 2022.

[28] M. Tanveer, A. Badshah, H. Alasmary, and S. A. Chaudhry, "CMAF-IIoT: Chaotic map-based authentication framework for industrial internet of things," *Internet of Things*, vol. 23, 100902, 2023.

[29] Y. Zhang, D. He, P. Vijayakumar, M. Luo, and X. Huang, "Sapfs: An efficient symmetric-key authentication key agreement scheme with perfect forward secrecy for industrial internet of things," *IEEE Internet Things J.*, 2023.

[30] A. Devi, A. Kumar, G. Rathee, and H. Saini, "User authentication of Industrial Internet of Things (IIoT) through Blockchain," *Multimed. Tools Appl.*, vol. 82, no. 12, pp. 19021–19039, 2023.

[31] W. Ali and A. A. Ahmed, "An authenticated group shared key mechanism based on a combiner for hash functions over the industrial internet of things," *Processes*, vol. 11, no. 5, 1558, 2023.

[32] S. Hussain and S. A. Chaudhry, "Comments on 'biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment,'" *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10936–10940, 2019.

[33] R. Splinter, "eBiometrics: Data acquisition and Physiological Sensing," in *Proc. 2021 IEEE 18th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*, IEEE, 2021, pp. 112–115.

[34] H. Hamidi, "An approach to develop the smart health using internet of Things and authentication based on biometric technology," *Futur. Gener. Comput. Syst.*, vol. 91, pp. 434–449, 2019.

[35] A. Anand, S. Rani, D. Anand, H. M. Aljahdali, and D. Kerr, "An efficient CNN-based deep learning model to Detect Malware Attacks (CNN-DMA) in 5G-IoT healthcare applications," *Sensors*, vol. 21, no. 19, 6346, 2021.

[36] F. Farid, M. Elkhodr, F. Sabrina, F. Ahamed, and E. Gide, "A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services," *Sensors*, vol. 21, no. 2, 552, 2021.

[37] F. Ahamed, F. Farid, B. Suleiman, Z. Jan, L. A. Wahsheh, and S. Shahrestani, "An intelligent multimodal biometric authentication model for personalised healthcare services," *Futur. Internet*, vol. 14, no. 8, 222, 2022.

[38] H. Al-Assam, W. Hassan, and S. Zeadally, "Automated biometric authentication with cloud computing," *Biometric-Based Phys. cybersecurity Syst.*, pp. 455–475, 2019.

[39] Y. Liu, X. Hao, W. Ren, R. Xiong, T. Zhu, and K. R. Choo, "A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things," *IEEE Trans. Comput.*, vol. 72, no. 2, pp. 501–512, 2022.

[40] S. Kamil, M. Ayob, S. Abdullah, and Z. Ahmad, "Challenges in multi-layer data security for video steganography," *Asia-Pacific J. Inf. Technol. Multimed.*, vol. 7, no. 2–2, pp. 53–62, 2018.

[41] N. Odyuo, S. Lodh, and S. Walling, "Multifactor mutual authentication of IoT devices and server," in *Proc. 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, IEEE, 2023, pp. 391–396.

[42] C.-M. Chen, X. Li, S. Liu, M.-E. Wu, and S. Kumari, "Enhanced authentication protocol for the Internet of Things environment," *Secur. Commun. Networks*, 2022.

[43] R. Bułat and M. R. Ogiela, "Personalized context-aware authentication protocols in IoT," *Appl. Sci.*, vol. 13, no. 7, 4216, 2023.

[44] I. Alshawish and A. Al-Haj, "An efficient mutual authentication scheme for IoT systems," *J. Supercomput.*, vol. 78, no. 14, pp. 16056–16087, 2022.

[45] F. Chen, Z. Xiao, T. Xiang, J. Fan, and H.-L. Truong, "A full lifecycle authentication scheme for large-scale smart IoT applications," *IEEE Trans. Dependable Secur. Comput.*, 2022.

[46] Z. Chen, X. Feng, and S. Zhang, "Emotion detection and face recognition of drivers in autonomous vehicles in IoT platform," *Image Vis. Comput.*, vol. 128, 104569, 2022.

[47] S. Ahmad and B. Fuller, "Thirdeye: Triplet based iris recognition without normalization," in *Proc. 2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, IEEE, 2019.

[48] S. Minaee and A. Abdolrashidi, "Deepiris: Iris recognition using a deep learning approach," arXiv Prepr., arXiv1907.09380, 2019.

[49] M. B. Lee, Y. H. Kim, and K. R. Park, "Conditional generative adversarial network-based data augmentation for enhancement of iris recognition accuracy," *IEEE Access*, vol. 7, pp. 122134–122152, 2019.

[50] H. D. Rafik and M. Boubaker, "A multi biometric system based on the right iris and the left iris using the combination of convolutional neural networks," in *Proc. 2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS)*, IEEE, 2020.

[51] D. Samai, K. Bensid, A. Meraoumia, A. Taleb-Ahmed, and M. Bedda, "2D and 3D palmprint recognition using deep learning method," in *Proc. 2018 3rd international conference on pattern* analysis *and intelligent systems (PAIS)*, IEEE, 2018.

[52] D. Zhong, Y. Yang, and X. Du, "Palmprint recognition using siamese network," in *Proc. 13th Chinese Conference on Biometric Recognition, CCBR 2018*, Springer, 2018, pp. 48–55.

[53] M. Izadpanahkakhk, S. M. Razavi, M. Taghipour-Gorjikolaie, S. H. Zahiri, and A. Uncini, "Deep region of interest and feature extraction models for palmprint verification using convolutional neural networks transfer learning," *Appl. Sci.*, vol. 8, no. 7, 1210, 2018.

[54] H. Shao and D. Zhong, "Few-shot palmprint recognition via graph neural networks," *Electron. Lett.*, vol. 55, no. 16, pp. 890–892, 2019.

[55] H. Vadher, P. Patel, A. Nair, T. Vyas, S. Desai, L. Gohil, S. Tanwar, D. Garg, and A. Singh, "EEG-based biometric authentication system using convolutional neural network for military applications," *Secur. Priv.*, vol. 7, no. 2, e345, 2024.

[56] B.-H. Kim and J.-Y. Pyun, "ECG identification for personal authentication using LSTM-based deep recurrent neural networks," *Sensors*, vol. 20, no. 11, 3069, 2020.

[57] D. Jyotishi and S. Dandapat, "An ECG biometric system using hierarchical LSTM with attention mechanism," *IEEE Sens. J.*, vol. 22, no. 6, pp. 6052–6061, 2021.
[58] S. Zhao, B. Zhang, and C. L. P. Chen, "Joint deep convolutional feature representation for hyperspectral palmprint recognition," *Inf. Sci. (Ny).*, vol. 489, pp. 167–181, 2019.
[59] Z. Xie, Z. Guo, and C. Qian, "Palmprint gender classification by convolutional neural network," *IET Comput. Vis.*, vol. 12, no. 4, pp. 476–483, 2018.
[60] H. Qin, M. A. El-Yacoubi, Y. Li, and C. Liu, "Multi-scale and multi-direction GAN for CNN-based single palm-vein identification," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2652–2666, 2021.
[61] F. Wang, L. Leng, A. B. J. Teoh, and J. Chu, "Palmprint false acceptance attack with a Generative Adversarial Network (GAN)," *Appl. Sci.*, vol. 10, no. 23, 8547, 2020.
[62] D. Snyder, D. Garcia-Romero, G. Sell, D. Povey, and S. Khudanpur, "X-vectors: Robust dnn embeddings for speaker recognition," in *Proc. 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, IEEE, 2018, pp. 5329–5333.
[63] M. Ravanelli and Y. Bengio, "Learning speaker representations with mutual information," *Reports on Internet of Things*, vol. 2, no. 1, 2023.
[64] K. Aizat, O. Mohamed, M. Orken, A. Ainur, and B. Zhumazhanov, "Identification and authentication of user voice using DNN features and i-vector," *Cogent Eng.*, vol. 7, no. 1, 1751557, 2020.
[65] N. Jiang and T. Liu, "Research on voiceprint recognition of camouflage voice based on deep belief network," *Int. J. Autom. Comput.*, vol. 18, no. 6, pp. 947–962, 2021.
[66] S. Chen, H. Wen, J. Wu, A. Xu, Y. Jiang, H. Song, and Y. Chen, "Radio frequency fingerprint-based intelligent mobile edge computing for internet of things authentication," *Sensors*, vol. 19, no. 16, 3610, 2019.
[67] U. Elordi, C. Lunerti, L. Unzueta, J. Goenetxea, N. Aranjuelo, A. Bertelsen, and I. Arganda-Carreras, "Designing automated deployment strategies of face recognition solutions in heterogeneous IoT platforms," *Information*, vol. 12, no. 12, 532, 2021.
[68] S. Purnapatra, C. Miller-Lynch, S. Miner, Y. Liu, K. Bahmani, S. Dey, and S. Schuckers, "Presentation attack detection with advanced cnn models for noncontact-based fingerprint systems," in *2023 11th International Workshop on Biometrics and Forensics (IWBF)*, IEEE, pp. 1–6, 2023.
[69] R. Kumari and H. Garg, "CNN-based features fusion of knuckle and fingerprint for multimodal biometrics system," in *Proc. AIP Conference*, AIP Publishing, 2023.
[70] W. Yan, J. Tang, and S. Stucki, "Design and implementation of a lightweight deep CNN-based plant biometric authentication system," *IEEE Access*, 2023.
[71] K. K. Shinde and C. N. Kayte, "Fingerprint recognition based on deep learning pre-train with our best CNN model for person identification," *ECS Trans.*, vol. 107, no. 1, 2209, 2022.
[72] B. Nithya and P. Sripriya, "Fingerprint identification by training a LSTM Network with fingerprint segments as sequence inputs," in *Proc. 2021 6th International Conference on Communication and Electronics Systems (ICCES)*, IEEE, 2021, pp. 1773–1779.
[73] K. Tse and K. Hung, "Framework for user behavioural biometric identification using a multimodal scheme with keystroke trajectory feature and recurrent neural network on a mobile platform," *IET Biometrics*, vol. 11, no. 2, pp. 157–170, 2022.
[74] M. A.-N. I. Fahim and H. Y. Jung, "A lightweight GAN network for large scale fingerprint generation," *IEEE Access*, vol. 8, pp. 92918–92928, 2020.
[75] O. Striuk and Y. Kondratenko, "Adaptive deep convolutional GAN for fingerprint sample synthesis," in *Proc. 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT)*, IEEE, 2021, pp. 193–196.
[76] O.-A. Ugot, C. Yinka-Banjo, and S. Misra, "Biometric fingerprint generation using generative adversarial networks," in *Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities*, Springer, 2021, pp. 51–83.
[77] D. Wang, H. Yu, D. Wang, and G. Li, "Face recognition system based on CNN," in *Proc. 2020 International Conference on Computer Information and Big Data Applications (CIBDA)*, 2020, pp. 470–473. doi: 10.1109/CIBDA50819.2020.00111
[78] R. M. Riyaas and A. S. Alphonse, "Face recognition system based on novel Peak Response-based Sobel Directional Pattern (PRSDP) and the Stacked Restricted Boltzmann Machine (SRBM)," in *Proc. 2024 5th International Conference on Innovative Trends in Information Technology (ICITIIT)*, 2024, pp. 1–6. doi: 10.1109/ICITIIT61487.2024.10580819
[79] R. Hammouche, A. Attia, S. Akhrouf, and Z. Akhtar, "Gabor filter bank with deep autoencoder based face recognition system," *Expert Syst. Appl.*, vol. 197, 116743, 2022. doi: https://doi.org/10.1016/j.eswa.2022.116743
[80] S. Wang and S. Jia, "Signature handwriting identification based on generative adversarial networks," *Journal of Physics: Conference Series*, 42047, 2019.
[81] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Exploring recurrent neural networks for on-line handwritten signature biometrics," *IEEE Access*, vol. 6, pp. 5128–5138, 2018.
[82] N. Li, Z. Wang, X. Yang, Z. Zhang, W. Zhang, S. Sang, and H. Zhang, "Deep learning assisted thermogalvanic hydrogel e-skin for self-powered signature recognition and biometric authentication," *Adv. Funct. Mater.*, vol. 34, no. 18, 2314419, 2024.
[83] M. Singhal and K. Shinghal, "Secure deep multimodal biometric authentication using online signature and face features fusion," *Multimed. Tools Appl.*, vol. 83, no. 10, pp. 30981–31000, 2024. doi: 10.1007/s11042-023-16683-1
[84] M. Vijay and G. Indumathi, "Deep belief network-based hybrid model for multimodal biometric system for futuristic security applications," *J. Inf. Secur. Appl.*, vol. 58, 102707, 2021.
[85] U. M. Butt, F. Masood, Z. Unnisa, S. Razzaq, Z. Dar, S. Azhar, I. Abbas, and M. Ahmad, *A Deep Insight into Signature Verification Using Deep Neural Network BT - Intelligent Systems and Applications*, K. Arai, S. Kapoor, and R. Bhatia, Eds., Cham: Springer International Publishing, 2021, pp. 128–138.
[86] M. Jampour and M. Javidi, "A joint DNN architecture with explicit features for Signature Identification image," *J. Mach. Vis. Image Process.*, vol. 7, no. 2, pp. 57–69, 2021.
[87] G. Huo, Q. Zhang, Y. Zhang, Y. Liu, H. Guo, and W. Li, "Multi-source heterogeneous iris recognition using stacked convolutional deep belief networks-deep belief network model," *Pattern Recognit. Image Anal.*, vol. 31, pp. 81–90, 2021.
[88] C. Lin and A. Kumar, "Contactless and partial 3D fingerprint recognition using multi-view deep representation," *Pattern Recognit.*, vol. 83, pp. 314–327, 2018.
[89] S. Minaee and A. Abdolrashidi, "Finger-GAN: Generating realistic fingerprint images using connectivity imposed GAN," arXiv Prepr., arXiv1812.10482, 2018.
[90] E. Tabassi, T. Chugh, D. Deb, and A. K. Jain, "Altered fingerprints: Detection and localization," in *Proc. 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, IEEE, 2018.
[91] T. Oblak, R. Haraksim, L. Beslay, and P. Peer, "Probabilistic fingermark quality assessment with quality region localisation," *Sensors*, 2023. doi: 10.3390/s23084006
[92] T. Kang, K.-I. Oh, J.-J. Lee, B.-S. Park, W. Oh, and S.-E. Kim, "Measurement and analysis of human body channel response for biometric recognition," *IEEE Trans. Instrum. Meas.*, vol. 70, pp. 1–12, 2021. doi: 10.1109/TIM.2021.3106132
[93] E. M. Cherrat, R. Alaoui, and H. Bouzahir, "Convolutional neural networks approach for multimodal biometric identification system using the fusion of fingerprint, finger-vein and face images," *PeerJ Comput. Sci.*, vol. 6, e248, 2020.
[94] V. Anand and V. Kanhangad, "PoreNet: CNN-based pore descriptor for high-resolution fingerprint recognition," *IEEE Sens. J.*, vol. 20, no. 16, pp. 9305–9313, 2020.
[95] W. J. Wong and S.-H. Lai, "Multi-task CNN for restoring corrupted fingerprint images," *Pattern Recognit.*, vol. 101, 107203, 2020.
[96] A. Chowdhury, S. Kirchgasser, A. Uhl, and A. Ross, "Can a CNN automatically learn the significance of minutiae points for fingerprint matching?" in *Proc. the IEEE/CVF Winter Conference on Applications of Computer Vision*, 2020, pp. 351–359.
[97] Y. Zhang, S. Pan, X. Zhan, Z. Li, M. Gao, and C. Gao, "Fldnet: Light dense cnn for fingerprint liveness detection," *IEEE Access*, vol. 8, pp. 84141–84152, 2020.
[98] S. J. J. Arputhamoni and A. G. Saravanan, "Online smart voting system using biometrics based facial and fingerprint detection on image processing and CNN," in *Proc. 2021 Third International*

Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), IEEE, 2021.
[99] S. Barzut, M. Milosavljević, S. Adamović, M. Saračević, N. Maček, and M. Gnjatović, "A novel fingerprint biometric cryptosystem based on convolutional neural networks," *Mathematics*, vol. 9, no. 7, 730, 2021.
[100] C. Yuan, Q. Cui, X. Sun, Q. M. J. Wu, and S. Wu, "Fingerprint liveness detection using an improved CNN with the spatial pyramid pooling structure," in *Advances in Computers*, Elsevier, 2021, vol. 120, pp. 157–193.
[101] P. Nahar, N. S. Chaudhari, and S. K. Tanwani, "Fingerprint classification system using CNN," *Multimed. Tools Appl.*, vol. 81, no. 17, pp. 24515–24527, 2022.
[102] W. Yang, S. Wang, G. Zheng, J. Yang, and C. Valli, "A privacy-preserving lightweight biometric system for internet of things security," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 84–89, 2019.
[103] R. Kumar, "Internet of things for the prevention of black hole using fingerprint authentication and genetic algorithm optimization," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 8, 17, 2018.
[104] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," *Internet Things Cyber-Physical Syst.*, vol. 3, pp. 280–308, 2023.
[105] B. Li, Y. Feng, Z. Xiong, W. Yang, and G. Liu, "Research on AI security enhanced encryption algorithm of autonomous IoT systems," *Inf. Sci. (Ny).*, vol. 575, pp. 379–398, 2021.
[106] Y. Moon, I. Ryoo, and S. Kim, "Face antispoofing method using color texture segmentation on FPGA," *Secur. Commun. Networks*, vol. 2021, 9939232, 2021. doi: 10.1155/2021/9939232
[107] Z. Zhang, H. Ning, F. Farha, J. Ding, and K.-K. R. Choo, "Artificial intelligence in physiological characteristics recognition for internet of things authentication," *Digit. Commun. Networks*, 2022.
[108] F. Wang, J. Cheng, W. Liu, and H. Liu, "Additive margin softmax for face verification," *IEEE Signal Process. Lett.*, vol. 25, no. 7, pp. 926–930, 2018.
[109] H. Wang, Y. Wang, Z. Zhou, X. Ji, D. Gong, J. Zhou, Z. Li, and W. Liu, "Cosface: Large margin cosine loss for deep face recognition," in *Proc. the IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp. 5265–5274.
[110] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "Arcface: Additive angular margin loss for deep face recognition," in *Proc. the IEEE Conference on Computer Vision and Pattern Recognition*, 2019, pp. 4690–4699.
[111] X. Zhang, R. Zhao, Y. Qiao, X. Wang, and H. Li, "Adacos: Adaptively scaling cosine logits for effectively learning deep face representations," in *Proc. the IEEE Conference on Computer Vision and Pattern Recognition*, 2019, pp. 10823–10832.
[112] X. Zhang, R. Zhao, J. Yan, M. Gao, Y. Qiao, X. Wang, and H. Li, "P2sgrad: Refined gradients for optimizing deep face models," in *Proc. the IEEE Conference on Computer Vision and Pattern Recognition*, 2019, pp. 9906–9914.
[113] Y. Duan, J. Lu, and J. Zhou, "Uniformface: Learning deep equidistributed representation for face recognition," in *Proc. the IEEE Conference on Computer Vision and Pattern Recognition*, 2019, pp. 3415–3424.
[114] H. Liu, X. Zhu, Z. Lei, and S. Z. Li, "Adaptiveface: Adaptive margin and sampling for face recognition," in *Proc. the IEEE Conference on Computer Vision and Pattern Recognition*, 2019, pp. 11947–11956.
[115] R. Ranjan, C. D. Castillo, and R. Chellappa, "L2-constrained softmax loss for discriminative face verification," arXiv Prepr., arXiv1703.09507, 2017.
[116] S. Minaee and A. Abdolrashidi, "Iris-gan: Learning to generate realistic iris images using convolutional gan," arXiv Prepr., arXiv1812.04822, 2018.
[117] M. G. Alaslani, "Convolutional neural network based feature extraction for iris recognition," *Int. J. Comput. Sci. Inf. Technol. Vol*, vol. 10, 2018.
[118] H. Hofbauer, E. Jalilian, and A. Uhl, "Exploiting superior CNN-based iris segmentation for better recognition accuracy," *Pattern Recognit. Lett.*, vol. 120, pp. 17–23, 2019.
[119] Z. D. P. Xin, P. Xin, L. Xiaoling, and G. Xiaojing, "Palmprint recognition based on deep learning," in *Proc. 6th International Conference on Wireless, Mobile and Multi-Media (ICWMMN 2015)*, 2015.
[120] H. Shao, D. Zhong, and X. Du, "Efficient deep palmprint recognition via distilled hashing coding," in *Proc. the IEEE Conference on Computer Vision and Pattern Recognition*, 2019, pp. 714–723.
[121] H. Shao, D. Zhong, and X. Du, "Cross-domain palmprint recognition based on transfer convolutional autoencoder," in *Proc. 2019 IEEE International Conference on Image Processing (ICIP)*, IEEE, 2019, pp. 1153–1157.
[122] J. Zhang, W. Yu, X. Yang, and F. Deng, "Few-shot learning for ear recognition," in *Proc. the 2019 International Conference on Image, Video and Signal Processing*, 2019, pp. 50–54.
[123] A. Sulavko, "Biometric-based key generation and user authentication using acoustic characteristics of the outer ear and a network of correlation neurons," *Sensors*, vol. 22, no. 23, 9551, 2022.
[124] S. Dodge, J. Mounsef, and L. Karam, "Unconstrained ear recognition using deep neural networks," *IET Biometrics*, vol. 7, no. 3, pp. 207–214, 2018.
[125] Ž. Emeršič, N. O. Playà, V. Štruc, and P. Peer, "Towards accessories-aware ear recognition," in *Proc. 2018 IEEE International Work Conference on Bioinspired Intelligence (IWOBI)*, IEEE, pp. 1–8, 2018.
[126] H. Sinha, R. Manekar, Y. Sinha, and P. K. Ajmera, "Convolutional neural network-based human identification using outer ear images," in *Proc. International Conference on Soft Computing for Problem Solving: SocProS 2017*, Springer, 2019, pp. 707–719.
[127] I. Omara, X. Wu, H. Zhang, Y. Du, and W. Zuo, "Learning pairwise SVM on hierarchical deep features for ear recognition," *IET Biometrics*, vol. 7, no. 6, pp. 557–566, 2018.
[128] E. E. Hansley, M. P. Segundo, and S. Sarkar, "Employing fusion of learned and handcrafted features for unconstrained ear recognition," *IET Biometrics*, vol. 7, no. 3, pp. 215–223, 2018.
[129] X. Chen, J. Weng, W. Lu, and J. Xu, "Multi-gait recognition based on attribute discovery," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 40, no. 7, pp. 1697–1710, 2017.
[130] F. Battistone and A. Petrosino, "TGLSTM: A time based graph deep learning approach to gait recognition," *Pattern Recognit. Lett.*, vol. 126, pp. 132–138, 2019.
[131] Q. Zou, Y. Wang, Q. Wang, Y. Zhao, and Q. Li, "Deep learning-based gait recognition using smartphones in the wild," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3197–3212, 2020.
[132] 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, 2018.
[133] Q. Zhang, D. Zhou, and X. Zeng, "HeartID: A multiresolution convolutional neural network for ECG-based biometric human identification in smart health applications," *IEEE Access*, vol. 5, pp. 11805–11816, 2017.
[134] Z. Zhao, Y. Zhang, Y. Deng, and X. Zhang, "ECG authentication system design incorporating a convolutional neural network and generalized s-transformation," *Comput. Biol. Med.*, vol. 102, pp. 168–179, 2018.
[135] S. M. Mathews, C. Kambhamettu, and K. E. Barner, "A novel application of deep learning for single-lead ECG classification," *Comput. Biol. Med.*, vol. 99, pp. 53–62, 2018.
[136] T. Golany, G. Lavee, S. T. Yarden, and K. Radinsky, "Improving ECG classification using generative adversarial networks," in *Proc. the AAAI Conference on Artificial Intelligence*, 2020, pp. 13280–13285.
[137] V. K. N. K. Pai, M. Balrai, S. Mogaveera, and D. Aeloor, "Face recognition using convolutional neural networks," in *Proc. 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, 2018, pp. 165–170.
[138] S. D. Lin and K. Chen, "Illumination invariant thermal face recognition using convolutional neural network," in *Proc. 2019 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, IEEE, 2019, pp. 83–84.
[139] T. Phillips, X. Zou, F. Li, and N. Li, "Enhancing biometric-capsule-based authentication and facial recognition via deep learning," in *Proc. the 24th ACM Symposium on Access Control Models and Technologies*, 2019, pp. 141–146.
[140] S. Khan, M. H. Javed, E. Ahmed, S. A. A. Shah, and S. U. Ali, "Facial recognition using convolutional neural networks and implementation on smart glasses," in *Proc. 2019 International*

Conference on Information Science and Communication Technology (ICISCT), IEEE, 2019.
[141] A. B. Perdana and A. Prahara, "Face recognition using light-convolutional neural networks based on modified VGG16 model," in *Proc. 2019 International Conference of Computer Science and Information Technology (ICoSNIKOM)*, IEEE, 2019.
[142] X. Liu, Z. Guo, J. You, and B. V. K. V. Kumar, "Dependency-aware attention control for image set-based face recognition," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1501–1512, 2019.
[143] F. Zhao, J. Li, L. Zhang, Z. Li, and S.-G. Na, "Multi-view face recognition using deep neural networks," *Futur. Gener. Comput. Syst.*, vol. 111, pp. 375–380, 2020.
[144] F. I. Eyiokur, D. Yaman, and H. K. Ekenel, "Domain adaptation for ear recognition using deep convolutional neural networks," *IET Biometrics*, vol. 7, no. 3, pp. 199–206, 2018.
[145] A. Abd Almisreb, N. Jamil, and N. M. Din, "Utilizing AlexNet deep transfer learning for ear recognition," in *Proc. 2018 Fourth International Conference on Information Retrieval and Knowledge Management (CAMP)*, IEEE, pp. 1–5, 2018.
[146] S. Minaee, E. Azimi, and A. Abdolrashidi, "Fingernet: Pushing the limits of fingerprint recognition using convolutional neural network," arXiv Prepr., arXiv1907.12956, 2019.
[147] Y. Mao and T.-C. Chang, "Automatic electrocardiogram sensing classifier based on improved backpropagation neural network," *Sensors Mater.*, vol. 32, 2020.
[148] K. Jafarian, V. Vahdat, S. Salehi, and M. Mobin, "Automating detection and localization of myocardial infarction using shallow and end-to-end deep neural networks," *Appl. Soft Comput.*, vol. 93, 106383, 2020.
[149] Z. Xu, W. Lu, Q. Zhang, Y. Yeung, and X. Chen, "Gait recognition based on capsule network," *J. Vis. Commun. Image Represent.*, vol. 59, pp. 159–167, 2019.
[150] J. Su, Y. Zhao, and X. Li, "Deep metric learning based on center-ranked loss for gait recognition," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, IEEE, 2020, pp. 4077–4081.
[151] X. Wu, T. Yang, and Z. Xia, "Gait recognition based on densenet transfer learning," *Int. J. Sci. Environ.*, vol. 9, pp. 1–14, 2020.
[152] H. Arshad, M. A. Khan, M. I. Sharif, M. Yasmin, J. M. R. S. Tavares, Y. Zhang, and S. C. Satapathy, "A multilevel paradigm for deep convolutional neural network features selection with an application to human gait recognition," *Expert Syst.*, vol. 39, no. 7, e12541, 2022.
[153] X. Wang and K. Yan, "Gait classification through CNN-based ensemble learning," *Multimed. Tools Appl.*, vol. 80, no. 1, pp. 1565–1581, 2021.
[154] T. Huynh-The, C.-H. Hua, N. A. Tu, and D.-S. Kim, "Learning 3D spatiotemporal gait feature by convolutional network for person identification," *Neurocomputing*, vol. 397, pp. 192–202, 2020.
[155] K. Nguyen, C. Fookes, A. Ross, and S. Sridharan, "Iris recognition with off-the-shelf CNN features: A deep learning perspective," *IEEE Access*, vol. 6, pp. 18848–18855, 2017.
[156] M. Fan, Z. Liu, M. Xu, S. Wang, T. Zeng, X. Gao, L. Li, "Generative adversarial network-based super-resolution of diffusion-weighted imaging: Application to tumour radiomics in breast cancer," *NMR Biomed.*, vol. 33, no. 8, e4345, 2020.
[157] T. Le-Tien, H. Phan-Xuan, P. Nguyen-Duy, and L. Le-Ba, "Iris-based biometric recognition using modified convolutional neural network," in *Proc. 2018 International Conference on Advanced Technologies for Communications (ATC)*, IEEE, pp. 184–188, 2018.
[158] J. Jayanthi, E. L. Lydia, N. Krishnaraj, T. Jayasankar, R. L. Babu, and R. A. Suji, "An effective deep learning features based integrated framework for iris detection and recognition," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 3, pp. 3271–3281, 2021.
[159] P. Rodriguez, G. Cucurull, J. Gonzàlez, J. M. Gonfaus, K. Nasrollahi, T. B. Moeslund, "Deep pain: Exploiting long short-term memory networks for facial expression classification," *IEEE Trans. Cybern.*, vol. 52, no. 5, pp. 3314–3324, 2022. doi: 10.1109/TCYB.2017.2662199
[160] Y. Zheng, D. K. Pal, and M. Savvides, "Ring loss: Convex feature normalization for face recognition," in *Proc. the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 5089–5097, 2018.
[161] R. D. Labati, E. Muñoz, V. Piuri, R. Sassi, and F. Scotti, "Deep-ECG: Convolutional neural networks for ECG biometric recognition," *Pattern Recognit. Lett.*, vol. 126, pp. 78–85, 2019.
[162] S. Yang, Q. He, Y. Lu, and B. Chen, "Maximum entropy intrinsic learning for spiking networks towards embodied neuromorphic vision," *Neurocomputing*, vol. 610, 128535, 2024. https://doi.org/10.1016/j.neucom.2024.128535
[163] W. G. Hatcher and W. Yu, "A survey of deep learning: Platforms, applications and emerging research trends," *IEEE Access*, vol. 6, pp. 24411–24432, 2018. doi: 10.1109/ACCESS.2018.2830661
[164] G. K. Sidiropoulos and G. A. Papakostas, "Machine biometrics - Towards identifying machines in a smart city environment," in *Proc. 2021 IEEE World AI IoT Congress (AIIoT)*, pp. 197–201, 2021. doi: 10.1109/AIIoT52608.2021.9454230
[165] Y. Tang, F. Gao, J. Feng, and Y. Liu, "FingerNet: An unified deep network for fingerprint minutiae extraction," in *Proc. 2017 IEEE International Joint Conference on Biometrics (IJCB)*, IEEE, 2017, pp. 108–116.
[166] Y. Zhao, B. Hu, Y. Wang, X. Yin, Y. Jiang, and X. Zhu, "Identification of gastric cancer with convolutional neural networks: a systematic review," *Multimed. Tools Appl.*, vol. 81, no. 8, pp. 11717–11736, 2022. doi: 10.1007/s11042-022-12258-8
[167] X. Yu, Q. Zhou, S. Wang, and Y. D. Zhang, "A systematic survey of deep learning in breast cancer," *Int. J. Intell. Syst.*, vol. 37, no. 1, pp. 152–216, 2022. doi: 10.1002/int.22622
[168] A. Binder, S. Bach, G. Montavon, K. R. Müller, and W. Samek, "Layer-wise relevance propagation for deep neural network architectures," in *Lecture Notes in Electrical Engineering*, pp. 913–922, 2016. doi: 10.1007/978-981-10-0557-2_87
[169] S. C. Hagness, A. Taflove, and S. D. Gedney, "Front matter," in *Corrosion*, 1976. doi: 10.1016/B978-0-408-00109-0.50001-8
[170] Y. Bentur, I. Layish, A. Krivoy, M. Berkovitch, E. Rotman, S. B. Haim, Y. Yehezkelli, E. Kozer, "Civilian adult self injections of atropine - Trimedoxime (TMB4) auto-injectors," *Clin. Toxicol.*, vol. 44, no. 3, pp. 301–306, 2006. doi: 10.1080/15563650600584519
[171] T. Wolf, M. Babaee, and G. Rigoll, "Multi-view gait recognition using 3D convolutional neural networks," in *Proc. 2016 IEEE International Conference on Image Processing (ICIP)*, IEEE, 2016, pp. 4165–4169.
[172] F. de Melo, H. C. Neto, and H. P. da Silva, "System on Chip (SoC) for invisible Electrocardiography (ECG) biometrics," *Sensors*, 2022. doi: 10.3390/s22010348
[173] N. Mitro, K. Argyri, L. Pavlopoulos, D. Kosyvas, L. Karagiannidis, M. Kostovasili, F. Misichroni, E. Ouzounoglou, and A. Amditis, "AI-enabled smart wristband providing real-time vital signs and stress monitoring," *Sensors*, 2023. doi: 10.3390/s23052821
[174] G. Aquino, M. G. F. Costa, and C. F. F. Costa Filho, "Explaining one-dimensional convolutional models in human activity recognition and biometric identification tasks," *Sensors*, 2022. doi: 10.3390/s22155644
[175] H. Guo, Z. Wang, B. Wang, X. Li, and D. M. Shila, "Fooling a deep-learning based gait behavioral biometric system," in *Proc. 2020 IEEE Security and Privacy Workshops (SPW)*, 2020, pp. 221–227. doi: 10.1109/SPW50608.2020.00052
[176] K. Jun, D.-W. Lee, K. Lee, S. Lee, and M. S. Kim, "Feature extraction using an RNN autoencoder for skeleton-based abnormal gait recognition," *IEEE Access*, vol. 8, pp. 19196–19207, 2020. doi: 10.1109/ACCESS.2020.2967845
[177] L. Sun, Z. Zhong, Z. Qu, and N. Xiong, "PerAE: An effective personalized autoencoder for ECG-based biometric in augmented reality system," *IEEE J. Biomed. Heal. Informatics*, vol. 26, no. 6, pp. 2435–2446, 2022. doi: 10.1109/JBHI.2022.3145999
[178] S. Saponara, A. Elhanashi, and Q. Zheng, "Recreating fingerprint images by convolutional neural network autoencoder architecture," *IEEE Access*, vol. 9, pp. 147888–147899, 2021. doi: 10.1109/ACCESS.2021.3124746
[179] C. Lin and A. Kumar, "Multi-siamese networks to accurately match contactless to contact-based fingerprint images," in *Proc. 2017 IEEE International Joint Conference on Biometrics (IJCB)*, IEEE, 2017, pp. 277–285.
[180] A. Peña, I. Serna, A. Morales, J. Fierrez, A. Ortega, A. Herrarte, M. Alcantara, and J. Ortega-Garcia, "Human-centric multimodal machine learning: Recent advances and testbed on AI-based recruitment," *SN Comput. Sci.*, vol. 4, no. 5, 434, 2023.
[181] J. Ortega-Rodríguez, J. F. Gómez-González, and E. Pereda, "Selection of the minimum number of EEG sensors to guarantee biometric identification of individuals," *Sensors*, 2023. doi: 10.3390/s23094239

[182] M. Albaladejo-González, J. A. Ruipérez-Valiente, and F. Gómez Mármol, "Evaluating different configurations of machine learning models and their transfer learning capabilities for stress detection using heart rate," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 8, pp. 11011–11021, 2023.
[183] X. Zhang, Z. Fang, Y. Wen, Z. Li, and Y. Qiao, "Range loss for deep face recognition with long-tailed training data," in *Proc. the IEEE International Conference on Computer Vision*, 2017, pp. 5409–5418.
[184] B. Pandya, G. Cosma, A. A. Alani, A. Taherkhani, V. Bharadi, and T. M. McGinnity, "Fingerprint classification using a deep convolutional neural network," in *Proc. 2018 4th International Conference on Information Management (ICIM)*, IEEE, 2018, pp. 86–91.
[185] I. Rida, R. Herault, G. L. Marcialis, and G. Gasso, "Palmprint recognition with an efficient data driven ensemble classifier," *Pattern Recognit. Lett.*, vol. 126, pp. 21–30, 2019.
[186] J. S. Chung, A. Nagrani, and A. Zisserman, "Voxceleb2: Deep speaker recognition," arXiv Prepr., arXiv1806.05622, 2018.
[187] G. Bhattacharya, M. J. Alam, and P. Kenny, "Deep speaker recognition: Modular or monolithic?," in *Interspeech*, pp. 1143–1147, 2019.
[188] S. Shon, H. Tang, and J. Glass, "Frame-level speaker embeddings for text-independent speaker recognition and analysis of end-to-end model," in *Proc. 2018 IEEE Spoken Language Technology Workshop (SLT)*, 2018, IEEE, pp. 1007–1013.
[189] W. Cai, J. Chen, and M. Li, "Exploring the encoding layer and loss function in end-to-end speaker and language recognition system," arXiv Prepr., arXiv1804.05160, 2018.
[190] M. Hajibabaei and D. Dai, "Unified hypersphere embedding for speaker recognition," arXiv Prepr., arXiv1807.08312, 2018.
[191] W. Xie, A. Nagrani, J. S. Chung, and A. Zisserman, "Utterance-level aggregation for speaker recognition in the wild," in *Proc. 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, IEEE, 2019, pp. 5791–5795.
[192] V. L. F. Souza, A. L. I. Oliveira, and R. Sabourin, "A writer-independent approach for offline signature verification using deep convolutional neural networks features," in *Proc. 2018 7th Brazilian Conference on Intelligent Systems (BRACIS)*, IEEE, 2018, pp. 212–217.
[193] B. Maze, J. Adams, J. A. Duncan, N. Kalka, T. Miller, and C. Otto, "Iarpa janus benchmark-c: Face dataset and protocol," in *Proc. 2018 International Conference on Biometrics (ICB)*, IEEE, 2018, pp. 158–165.
[194] M. Pejic-bach, "Profiling intelligent systems applications in fraud detection and prevention: survey of research articles," in *Proc. 2010 International Conference on Intelligent Systems, Modelling and Simulation*, 2015. doi: 10.1109/ISMS.2010.26
[195] N. V Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic minority over-sampling technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.
[196] X. Wang, H. Wu, and Z. Yi, "Research on bank anti-fraud model based on k-means and hidden markov model," in *Proc. 2018 IEEE 3rd International Conference on Image, Vision and Computing (ICIVC)*, 2018, pp. 780–784. doi: 10.1109/ICIVC.2018.8492795
[197] M. Haghighat, M. Abdel-Mottaleb, and W. Alhalabi, "Discriminant correlation analysis: Real-time feature level fusion for multimodal biometric recognition," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 9, pp. 1984–1996, 2016.
[198] A. J. Prakash, K. K. Patro, S. Samantray, P. Pławiak, and M. Hammad, "A deep learning technique for biometric authentication using ECG beat template matching," *Information*, 2023. doi: 10.3390/info14020065
[199] J. Salas, F. B. Vidal, and F. Martinez-Trinidad, "Deep learning: Current state," *IEEE Lat. Am. Trans.*, vol. 17, no. 12, pp. 1925–1945, 2019. doi: 10.1109/TLA.2019.9011537
[200] Y. Wen, K. Zhang, Z. Li, and Y. Qiao, "A discriminative feature learning approach for deep face recognition," in *Proc. 14th European Conference on Computer vision–ECCV 2016*, Springer, 2016, pp. 499–515.
[201] S. S. Ali, V. S. Baghel, I. I. Ganapathi, and S. Prakash, "Robust biometric authentication system with a secure user template," *Image Vis. Comput.*, vol. 104, 104004, 2020.
[202] A. E. Orhan, "Self-supervised learning through the eyes of a child," *Advances in Neural Information Processing Systems*, pp. 9960–9971, 2020.