AI-powered biometrics for Internet of Things security: A review and future vision

Article *in* Journal of Information Security and Applications · March 2024

DOI: 10.1016/j.jisa.2024.103748

Ali Ismail Awad
United Arab Emirates University
99 PUBLICATIONS **3,030** CITATIONS

Aiswarya Babu
Khalifa University
5 PUBLICATIONS **23** CITATIONS

Ezedin Barka
United Arab Emirates University
84 PUBLICATIONS **1,588** CITATIONS

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

AI-powered biometrics for Internet of Things security: A review and future vision

Ali Ismail Awad [a,b,c,*], Aiswarya Babu [d,e], Ezedin Barka [a], Khaled Shuaib [a]

[a] College of Information Technology, United Arab Emirates University, Al Ain P.O. Box 15551, United Arab Emirates
[b] Big Data Analytics Center, United Arab Emirates University, Al Ain P.O. Box 15551, United Arab Emirates
[c] Faculty of Engineering, Al-Azhar University, Qena P.O. Box 83513, Egypt
[d] Advanced Research and Innovation Center, Khalifa University, Abu Dhabi P.O. Box 127788, United Arab Emirates
[e] Department of Aerospace Engineering, Khalifa University, Abu Dhabi P.O. Box 127788, United Arab Emirates

ARTICLE INFO

Keywords:
Biometrics
Internet of Things
Artificial intelligence
Intelligent biometrics
Biometric authentication
Fingerprint authentication
Facial recognition
IoT security

ABSTRACT

Biometrics is a set of advanced technologies that use the physical or behavioral characteristics of individuals to provide reliable access control. With the rapid development in information and communication technology, biometrics has become an increasingly important field, especially with the integration of artificial intelligence (AI). Fingerprint- and facial-recognition technologies have been significantly improved by the use of AI. The widespread use of the Internet of Things (IoT) has led to security challenges and created new opportunities for biometrics to be used in various applications. This review provides a comprehensive analysis of intelligent or AI-powered biometrics, focusing on the integration of AI and biometrics for building security measures to improve IoT security. Due to their enhanced security and usability, biometric-based authentication methods are becoming increasingly popular in IoT environments. AI algorithms are essential for improving biometric systems in IoT applications by enabling advanced pattern recognition and adaptive decision-making. Furthermore, the integration of biometrics with AI and the IoT can help mitigate security risks, ensuring the protection of data and user privacy. This review makes three main contributions: it provides a comprehensive analysis of the interdependencies between the AI, biometrics, and IoT domains; it covers the applications of AI and biometrics in the context of the IoT; and it highlights the current challenges and future research directions for the deployment of intelligent biometrics in various IoT application domains. Furthermore, this review facilitates further research in the area of the application of intelligent biometrics in IoT applications.

1. Introduction

Biometrics is a set of technologies in which unique human physiological or behavioral traits are employed to establish strong access-control systems that fulfill the need for secure authentication and verification of individuals. By using biometric characteristics such as fingerprints, iris patterns, facial features, voice characteristics, and DNA, biometric systems can ensure reliable and secure identification of an individual, eliminating the need for traditional methods such as passwords, personal identification numbers (PINs), or smart cards. With the rapid development of information and communication technology, biometric technologies are in increasingly high demand for a wide variety of applications [1–3].

The Internet of Things (IoT) refers to a computing paradigm comprising a distributed network of devices that can sense physical properties and collect, process, or exchange data over the Internet. It is a constantly evolving technology that has become a key enabler in several critical fields, such as Industry 4.0, the Internet of Medical/Healthcare Things [4], smart cities, and other smart environments. Although IoT applications have added convenience, automation, and intelligence to people's daily lives, they have also created vulnerabilities that need to be addressed with robust, effective, and intelligent security measures [5–7].

Recent studies have shown the importance of biometrics in IoT security. Recent studies, such as that of Yang et al. [8], have found that biometric authentication offers improved security and usability in IoT environments. Biometric traits provide a highly accurate and reliable way to verify an individual's identity [9,10]. This makes biometric authentication an attractive solution for preventing identity theft, protecting against unauthorized access, and preventing data breaches in IoT systems.

[*] Corresponding author at: College of Information Technology, United Arab Emirates University, Al Ain P.O. Box 15551, United Arab Emirates.
E-mail addresses: ali.awad@uaeu.ac.ae (A.I. Awad), aiswarya.babu@ku.ac.ae (A. Babu), ebarka@uaeu.ac.ae (E. Barka), k.shuaib@uaeu.ac.ae (K. Shuaib).

https://doi.org/10.1016/j.jisa.2024.103748

Available online 21 March 2024

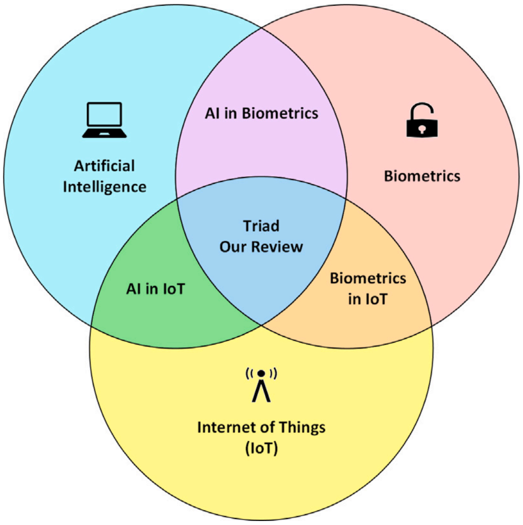

Fig. 1. Schematic Venn diagram illustrating the intersections of the AI, biometrics, and IoT domains, showing the core of this review.

The application of biometrics in IoT systems also offers benefits beyond security: it provides convenience and usability for the users of such systems. Biometric traits are inherent to individuals, eliminating the need to remember complex passwords or other complicated authentication schemes. This provides a seamless and user-friendly experience, encouraging widespread adoption of biometrics in IoT ecosystems.

Incorporating biometrics into IoT systems can help to address privacy concerns. Biometric authentication is privacy-preserving, and its templates and generated hashes can be securely stored and processed locally on IoT devices, as noted by Yang et al. [9] and Hussain and Chaudhry [11]. This reduces the risks associated with centralized databases and their increased potential for unauthorized access to personal information.

Artificial intelligence (AI) is a set of highly transformative technologies that is currently revolutionizing a diverse variety of sectors. As a result, ensuring robust security measures has become increasingly crucial. The evolution of authentication measures from traditional passwords and cryptographic keys to advanced authentication techniques has ensured accessible, secure, and more reliable means of data protection. Therefore, it is evident that there is a growing interest in integrating AI into biometrics and the IoT to improve the overall security posture and preserve data privacy [12,13].

AI algorithms can play a key role in enhancing biometric systems in general, and in IoT applications in particular. Integrating AI techniques such as machine learning (ML) and deep learning (DL) into biometric authentication can improve its accuracy and adaptability [14]. As noted by Jiang et al. [15], AI algorithms enable advanced pattern recognition, anomaly detection, and adaptive decision-making, allowing IoT users and devices to perform authentication more efficiently and securely.

This report closes a research gap by specifically reviewing the triad of AI, biometrics, and the IoT, highlighting the importance of biometrics in improving security, authentication, and the user experience in IoT systems and applications. The review focuses only on two biometric modalities – fingerprints and facial recognition – as these are the two most common and convenient biometric identifiers [3,16]. By addressing challenges and exploring opportunities, this review contributes to the development of secure and trustworthy biometrics-integrated IoT systems powered with AI to achieve enhanced security and reliability.

The review starts by providing a comprehensive overview of the background relating to biometric technologies and the IoT, discussing the need for IoT security and the importance of effective authentication. Next, biometrics and its relevance to IoT security are introduced, emphasizing its benefits. A discussion is also presented regarding the way in which AI – when integrated into biometrics – provides great advantages for IoT security. Furthermore, the paper presents the contributions of research in this area to addressing current IoT-based security challenges, improving user authentication through biometrics and AI, and exploring potential solutions. Finally, descriptive and exploratory analyses of the findings are presented to determine useful relations between biometric methods and algorithms for biometric detection, recognition, and performance-evaluation metrics.

This work supports the development and advancement of the three aspects of a triad – AI, biometrics, and the IoT – and their new interdisciplinary domain of opportunities. By examining AI-powered and -enhanced biometrics for the IoT, this review seeks to illuminate the advances and possibilities in this area that can improve security, privacy, and the user experience in the rapidly expanding world of the IoT.

1.1. Paper contributions

This review paper contributes to the existing body of knowledge by providing a comprehensive analysis of the integration of AI and biometrics – referred to as AI-powered or intelligent biometrics – within the context of the IoT. It offers insights into the current contributions, challenges, and future trends in this field, paving the way for further research and development in this area. A schematic showing the scope of the review and the intersections of the AI, biometrics, and IoT domains is shown in Fig. 1. The main contributions of this paper can be summarized by the following points.

- *Comprehensive analysis.* A systematic review of the literature is presented, analyzing a wide range of research articles, conference papers, and other scholarly works. This comprehensive analysis provides a holistic understanding of the integration of AI, biometrics, and the IoT.
- *Identification of potential contributions.* The current contributions of biometrics and AI-powered biometrics in various IoT domains, such as healthcare and smart cities, are identified. The paper highlights how these technologies can improve efficiency, safety, and quality of life.
- *Examining challenges.* The challenges associated with the integration of AI, biometrics, and the IoT, such as security, privacy, interoperability, and ethical considerations, are discussed. The review provides insights into open challenges that need to be addressed for successful integration.
- *Future trends and visions.* Future trends and visions in the integration of AI, the IoT, and biometrics are explored. Advances in wearable electronics, personalized healthcare, continuous authentication, infrastructure and health monitoring, ethical considerations, and energy management are discussed.

This deep exploration of the state of the art revealed that there have been several review studies, but none of these has comprehensively covered the triad of AI, biometrics, and the IoT. Section 2 provides more information about the previously published reviews and emphasizes the relevance of this work.

1.2. Paper structure

The review is structured in a manner that presents a clear overview, in-depth details, and the solutions offered for the triad of domains the upon which it is focused. The remainder of this paper is structured as follows. Section 2 provides an initial summary of related review papers. Section 3 offers an overview of the research methodology used in this review, and Section 4 provides a background base for the three domains – AI, biometrics, and the IoT – and their interconnects. Section 5 is the main focus of the paper, and this provides a detailed review of the interdependencies among the three domains. Current open challenges

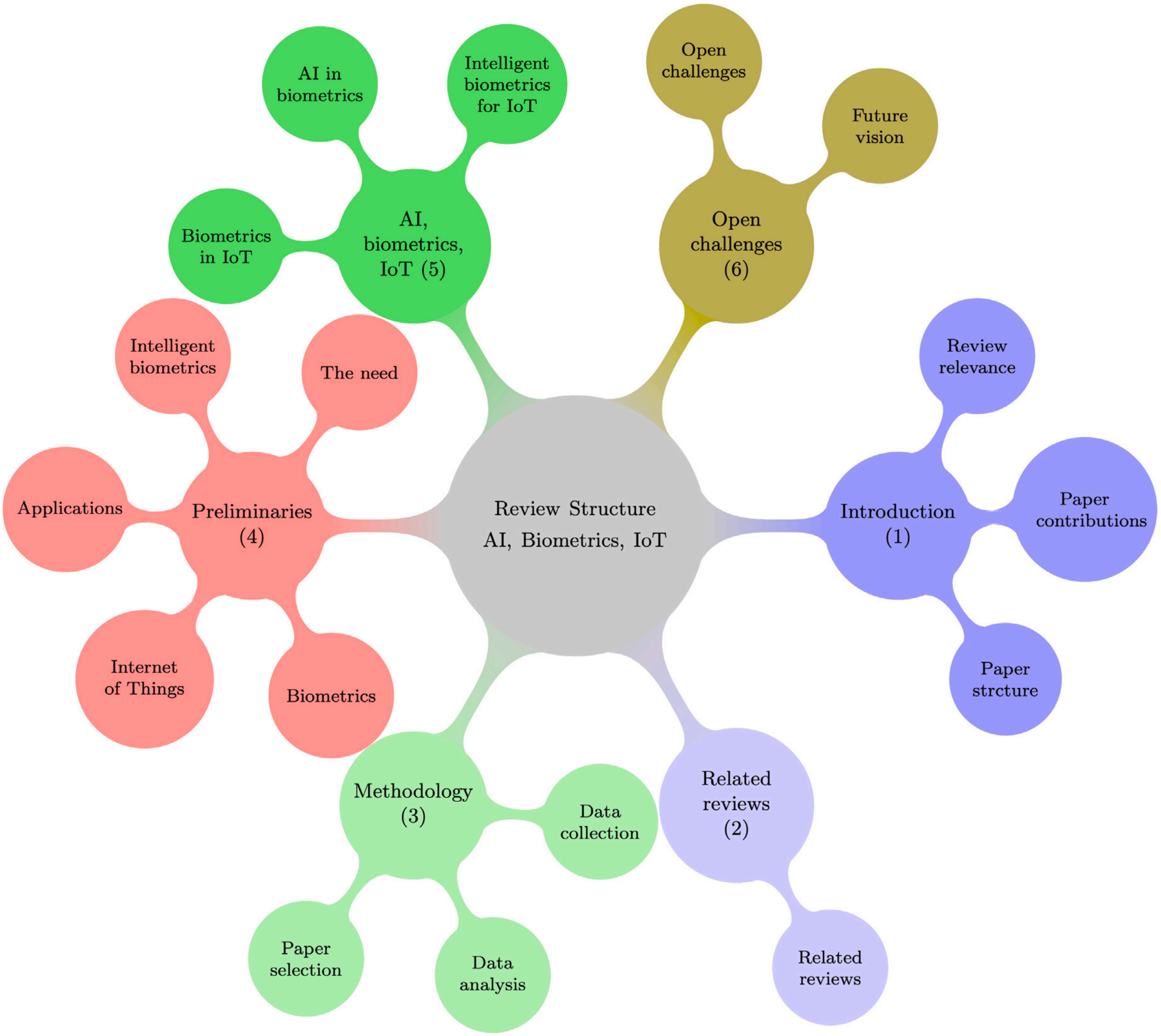

Fig. 2. Mind map showing the main topics and key concepts covered in this review.

and insights into the future directions and possible subsequent research opportunities are covered in Section 6. Lastly, Section 7 presents the conclusions of this review. A detailed mind map for this review showing the key areas introduced in the study is provided in Fig. 2.

2. Related reviews

Recently, research on the use of biometrics as a reliable access-control mechanism in IoT systems for enhancing security and accessibility through the application of various AI techniques has gained traction. Biometric data such as fingerprints and facial features are commonly employed to meet the requirements for establishing secure IoT platforms aided by AI. Consequently, the convergence of these three sectors holds tremendous potential for notable advances and exploratory opportunities. Table 1 provides an overview of the previously published articles in this domain and highlights the areas and sub-areas they have covered that are related to the scope of our review.

The review by Yang et al. [8] comprehensively explores the use of biometrics for enhancing security in the IoT, particularly regarding authentication and encryption. It provides insights into the current status of biometric-based authentication and biometric-based cryptographic systems, identifies implementation challenges, and highlights the advantages of using biometrics in IoT systems. However, it lacks an in-depth exploration of the interdependencies of the two domains. The work of Tomicic et al. [17] offers an overview of the soft biometric characteristics applicable to the IoT domain. It underscores the significance of integrating biometrics into the development of IoT devices and explores various soft biometric traits encompassing physical, behavioral, and environmental factors. The study suggests potential applications such as authentication, identification, and tracking within the IoT. However, it lacks an in-depth analysis of specific soft biometric traits and their implementation challenges; its focus on soft biometrics also limits the exploration of other relevant biometric modalities. Gayathri et al. [18] also provide a comprehensive review of various biometric techniques and their applications in the field of the IoT. Nonetheless, this lacks in-depth analysis and discussion of security issues and application areas, and there is also no discussion of the use of AI for improving biometric authentication in IoT-based applications.

Junaid et al. [19] examine in depth the intersection of AI, sensors, and vital health signs. However, their review has limited coverage of other biometric aspects, and it has some shortcomings in terms of providing a comprehensive analysis. A focus on biometric systems based on iris-image processing is given by Khoirunnisaa et al. [20], although this lacks a broader perspective on other biometric modalities and their integration with the IoT. A report by Xue et al. [21] presents a biometric-based authentication scheme for IoT-device identity. However, a potential drawback of this work is its lack of extensive analysis of potential security challenges of the proposed scheme and its limitations. The work carried out by Alsellami and Deshmukh [23] examines

Table 1
Summary of the reviews considering state-of-the-art research, highlighting the scopes, contexts, and main contributions of each. Definitions: ● indicates an area that is fully covered, ◑ indicates an area that is partially covered, and □ indicates an area that is not covered.

Ref.	Overall scope			AI		Biometrics		IoT			Contributions
	AI	Biometrics	IoT	DL	ML	Fingerprint	Face	Challenges	Solutions	Future vision	
[8]	◑	●	●	□	◑	●	□	●	●	◑	Review and insights
[17]	□	●	●	□	□	◑	●	◑	●	□	Review and challenges
[18]	◑	●	●	●	□	●	●	●	◑	◑	Overview insights and review
[19]	●	◑	◑	●	●	◑	□	●	◑	◑	Challenges and insights
[20]	◑	●	□	□	◑	□	◑	□	◑	◑	Review and insights
[21]	◑	●	●	□	□	●	◑	◑	●	◑	Challenges and solutions
[22]	◑	◑	●	◑	□	□	◑	●	●	◑	Security features
[23]	◑	●	●	□	◑	●	●	◑	●	◑	Biometrics exploration of other fields
[24]	●	◑	●	◑	●	◑	□	●	●	◑	AI and IoT solutions
[25]	◑	●	□	□	◑	●	●	□	□	◑	Scope of biometric systems
[26]	□	●	●	□	□	●	●	◑	●	◑	Biometrics in IoT
[27]	□	◑	●	□	□	◑	□	●	●	◑	Biomedical IoT
[28]	◑	●	●	□	□	●	●	●	●	◑	Biometrics in IoT security
[29]	●	□	●	◑	◑	□	□	●	●	◑	AI in IoT wearables
[30]	●	◑	◑	●	●	□	◑	◑	●	◑	AI in consumer research
[31]	◑	◑	●	□	◑	□	□	●	●	◑	IoT in smart clothing
[32]	●	◑	●	◑	◑	●	●	□	●	◑	Physiological authentication using AI
[33]	◑	●	◑	◑	◑	□	□	◑	●	◑	Focuses on behavioral biometrics in general
Our Review	●	●	●	●	●	●	●	●	●	●	Triad: AI, biometrics, and the IoT

recent trends in biometric-trait authentication within the IoT. However, the potential drawbacks of this work include its limited coverage of implementation challenges and its lack of detailed analysis of specific authentication techniques.

The review of Mukhopadhyay et al. [24] focuses on AI-based sensors for IoT applications. However, this appears to overlook the specific role of biometrics in enhancing security and authentication in IoT systems. Zhang et al. [25] provide an in-depth overview of biometric systems, their characteristics, solutions, and future insights. However, as an editorial piece, it lacks the depth of analysis found in research-focused papers. Although Ross et al. [26] briefly discuss digital forensic schemes for biometric data in smart cities in their review, this does not explore broader aspects of biometric security and its integration with the IoT.

The review of Karthick et al. [27] addresses the challenges of biomedical instruments using the IoT; nonetheless, this work lacks an extensive analysis of biometric authentication techniques and their application in healthcare IoT scenarios. Moradi et al. [28] presents a review on the improvements in the security level of IoT systems provided by the use of biometric features. However, this suffers from limitations in terms of discussing specific implementation challenges and potential vulnerabilities. Similarly, Chawla [29] explore the intersection of AI, the IoT, and wearable technology in smart healthcare, but they do not cover the specific role of biometrics in ensuring secure healthcare applications in detail. Another similar paper is presented by Mariani et al. [30], who explore the application of AI in consumer and marketing research involving the application of wearables based on the IoT. They also discuss the role of biometrics in the security of IoT-based devices and the role of AI in enhancing security features through biometrics; hence, providing an AI-based point of view while stating examples of biometric applications in the field of the IoT.

Fernández-Caramés and Fraga-Lamas [31] discuss the integration of IoT technologies into clothing and textiles, exploring the sensors involved and their applications, along with the challenges and opportunities involved in creating intelligent connected e-textiles. Such clothing uses an integration of biometrics into the IoT while briefly involving the application of AI.

The application of AI to recognizing physiological characteristics in IoT authentication is explored by Zhang et al. [32]. This article focuses on the integration of AI techniques to establish personalized authentication based on distinct physiological characteristics such as fingerprints, facial features, and heart-rate patterns. This strategy presents a robust authentication approach that is aligned with the dynamic nature of the IoT. However, the study's limitations include potential data-availability constraints for AI model training, inadequate investigation of ethical and bias-related considerations in physiological recognition, and a lack of comprehensive analysis concerning scalability and practical-deployment challenges in IoT authentication.

In contrast, Liang et al. [33] focus on the dynamic landscape of user-authentication challenges. They discuss continuous monitoring and analysis of distinctive behavioral patterns exhibited by individuals, encompassing keystrokes, touch gestures, and voice patterns, thereby presenting a resilient authentication mechanism. By harnessing AI techniques such as ML and deep neural networks (DNNs), their research probes the adaptive potential of behavioral biometrics to address evolving usage patterns and to enhance security within the IoT era. Notably, the limitations of this study include potential restrictions arising from dataset availability, a requirement for a more thorough investigation of privacy concerns, and an emphasis on technical aspects that may overshadow practical-implementation hurdles and emerging technologies.

In summary, although the review papers discussed in this section delve into various facets of AI, biometrics, and the IoT, they each exhibit distinct limitations; these limitations include a constrained scope, a lack of thorough analysis, or an oversight of specific subdomains within the expansive realm of biometrics and the IoT. Consequently, our review distinguishes itself by its relevance and distinctiveness. Our review is dedicated to delivering a meticulous and all-encompassing analysis of the interconnected domains of AI, biometrics, and the IoT. It delves into their scope, presents comprehensive solutions, and anticipates future trajectories while elucidating the interplay between these three pivotal domains.

3. Review methodology

This section provides a detailed account of how the data were collected, analyzed, and interpreted to draw meaningful conclusions. The robustness and reliability of the findings depend on the clarity and appropriateness of the methodology. In the context of the reviewed research articles on biometrics in the IoT, the methodology sections play a significant role in enhancing the understanding of how each study was designed and executed.

As the integration of biometrics into the IoT presents unique challenges and opportunities, the authors of the present work adopted a clear methodology to explore the various aspects of this interdisciplinary field. The following stages were used for the review methodology.

- *Stage one: Paper search and selection.* We searched for and extracted papers that discuss the interdependencies of the three domains – the IoT, AI, and biometrics – in electronic databases, including Scopus, Elsevier, and Google Scholar. The search was conducted using combinations of keywords including "IoT", "IoT security", "authentication", "security", "biometrics", "biometric authentication", "artificial intelligence", "AI", "AI in biometrics", "biometrics in IoT", "machine learning", and "deep learning".
- *Stage two: Paper classification.* The selected papers were classified into three main categories – AI, the IoT, and biometrics – 'and they were subdivided into IoT security, fingerprint recognition, facial recognition, ML, DL, challenges in the IoT, IoT-based solutions, and future scope to segregate the papers accordingly.
- *Stage three: Paper reviews.* The review of the articles focused on the interdependencies of the three domains – AI, the IoT, and biometrics – while conducting an in-depth analysis within these domains. This included ML and DL methods, algorithms for biometric detection, recognition, evaluation and performance-evaluation metrics, IoT security, IoT challenges, and types of biometrics.
- *Stage four: Analysis of findings.* The analysis of the reviews, including the extent of the technological interdependency of the domains and their influences on each other, is introduced in Section 5.

To develop a complete picture, in this work, the limitations of previous studies are discussed and examined. The research findings are summarized, and future research directions are presented.

3.1. Data collection

Initially, a number of papers were gathered from a broad range of sources including Scopus, Google Scholar, ScienceDirect, IEEE Xplore, and SpringerLink using keywords including "artificial intelligence", "biometrics", "IoT", "IoT security", "IoT authentication", "biometric authentication", "authentication", "security", "biometric authentication", "AI", "AI in biometrics", "biometrics in IoT", "machine learning", and "deep learning". After evaluating more than 200 papers, we narrowed our focus to 75 that were closely aligned with our three core domains. Graphical representations presented in Fig. 3 reveal a scarcity of recent articles covering the full triad.

To provide an in-depth analysis of the triad, we investigated emerging domains, opening up a range of possibilities for the interdomains considered herein. We intentionally selected high-impact-factor journals, underscoring our commitment to offering impactful research and ensuring the inclusion of peer-reviewed studies for enhanced reliability. Our review acknowledges the high editorial standards and robust peer-review practices of the selected journals, which are essential for providing insights into a rapidly evolving field.

3.2. Data analysis

To narrow down the selection to include more relevant research work, we conducted an initial analysis after gathering the papers to gain a visual sense of the collected articles. After undertaking a segregation process to filter the selected papers, we obtained articles from high-impact-factor journals that were distributed in the interdependent domains of AI, the IoT, and biometrics, as depicted in Fig. 3a. The articles published in recent years were considered to reveal their technological relevance and advancement, and hence their distribution over the years is shown in Fig. 3b. Fig. 3c shows the distribution of the numbers of papers considered to be reviewed for the triad sections. Fig. 3d provides a visual distribution of the articles reviewed within "AI in biometrics" based on their year of publication. Similarly, Figs. 3e and 3f provide the distributions of the numbers of articles published each year based on the topics "biometrics in IoT" and "the AI, IoT, and biometrics triad", respectively. Fig. 3g provides the distributions of papers within each of the sections of the paper based on the type of biometric identifiers used. Fig. 3h presents the distribution of papers in the IoT application domains considered within this review.

3.3. Paper-selection criteria

In the process of the selection and segregation of articles, a systematic approach was followed to identify research papers relevant to the integration of AI, biometrics, and the IoT. A thorough literature search was conducted using various academic databases and scientific repositories to collect a wide range of publications related to the topic. The search criteria were carefully defined to ensure the inclusion of recent and high-impact studies.

The initial search resulted in a substantial number of papers. These were then filtered based on their relevance to the integration of AI, biometrics, and the IoT. The inclusion and exclusion criteria were clearly outlined to ensure the selection of papers that met the specific scope and objectives of the review. Only peer-reviewed articles, conference papers, and reputable sources were considered to ensure the quality and reliability of the selected studies.

To further refine the selection, the abstracts and key sections of the shortlisted articles were evaluated. The process focused on identifying studies that presented significant contributions, novel insights, and up-to-date information on the integration of AI, biometrics, and the IoT. Papers that provided valuable discussions on challenges, future trends, and practical applications were prioritized for inclusion.

The final set of articles was chosen for review after a rigorous evaluation process. The selected articles collectively offer a comprehensive and diverse perspective on the topic, forming a well-rounded analysis and synthesis of the current state, challenges, and future vision of the integration of AI, the IoT, and biometrics.

Finally, the paper-review process offers insights into a comprehensive analysis and synthesis of the selected literature on the integration of AI, biometrics, and the IoT. This section of the paper is structured in an informative flow that offers information on "biometrics in IoT", "AI in Biometrics", and "AI-powered biometrics for IoT".

4. Preliminary background

As outlined above, biometrics focuses on using the distinct physiological and behavioral characteristics of individuals to verify their identity; it has recently seen notable advances and widespread use across various applications. The emergence of the IoT and the integration of AI into biometric systems have sparked increasing interest in exploring the potential of AI-powered biometrics in the IoT domain.

Biometric authentication is emerging as a dependable solution to address IoT security concerns. Employing an individual's unique physiological or behavioral traits for identification can ensure efficient and secure authentication. Integrating AI into biometric authentication (AI-powered biometrics) has consistently improved the precision and efficiency of biometric capture devices.

AI algorithms, such as ML and DL, enable continuous refinement and analysis of large quantities of data from IoT devices, bolstering security measures against unauthorized access and reducing false-acceptance rates (FARs). AI-powered biometric authentication provides a more robust and reliable authentication mechanism that is challenging for hackers to circumvent.

The integration of AI into biometric security solutions has diverse application potential in a variety of industries. In healthcare, biometric authentication can play a vital role in controlling access to sensitive patient information. In financial services, behavioral biometrics can effectively detect fraudulent activity. Additionally, in the transportation sector, biometric authentication can aid in controlling access to critical hub stations and vehicles.

This section offers an overview of biometric technologies, the IoT, biometric applications to the IoT, AI-powered biometrics, and the convergence of AI, biometrics, and the IoT.

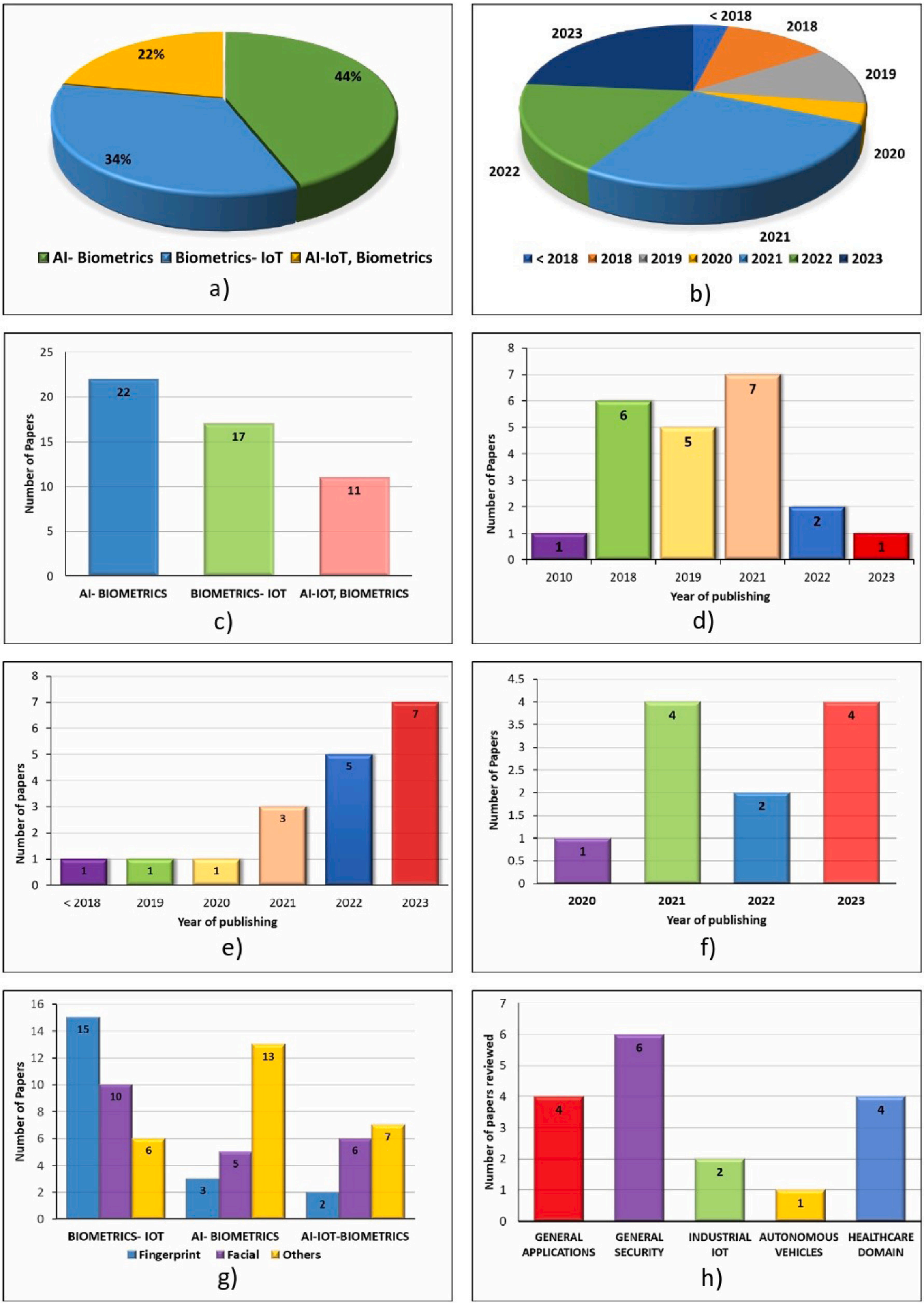

Fig. 3. Statistical analysis of the collected papers. (a) An overview of the collected papers. (b) Years of publication considered for the triad section. (c) Distribution of the reviewed papers per section or domain. (d) Paper distribution based on year of publication under "AI in biometrics". (e) Paper distribution based on year of publication under "biometrics in IoT". (f) Paper distribution based on year of publication under "the AI, IoT, and biometrics triad". (g) Paper distribution based on the type of biometrics, namely facial, fingerprint, or others. (h) Paper distribution based on the IoT application domain.

4.1. Biometric technologies

Biometrics has achieved widespread prominence as a reliable and secure access-control method that offers individual authentication and identification. Biometric solutions have been widely deployed across the IoT, primarily due to their remarkable ability to accurately identify individuals. As noted, these approaches are based on distinctive physiological or behavioral characteristics that are unique to each person, such as fingerprints, iris patterns, and facial features, making this a highly reliable method of verification when compared to traditional approaches [34]. Notably, the use of biometrics has proven particularly effective in fortifying security in IoT systems [35].

Biometric technologies include fingerprint scanning, facial recognition, iris scanning, and voice recognition; using these technologies, the unique traits of individuals can be used to identify them [36]. Of these methods, fingerprint scanning and facial recognition are frequently used because of their high accuracy and differentiation capabilities. Authentication – the process of confirming someone's identity when they are accessing a system or service – has increasingly embraced biometrics as a more secure and more reliable alternative to traditional methods such as passwords [37]. Consequently, biometric authentication has found extensive applications in industries such as finance, healthcare, and government, safeguarding sensitive data and transactions.

Key biometric-identification technologies include fingerprint, iris, facial, and voice recognition, and behavioral biometrics. Fingerprint recognition involves scanning and analyzing unique patterns on the fingers of a person to confirm their identity [37]. Iris recognition, which is typically based on near-infrared (NIR) light, captures a distinct image of the colored part of a person's eye; this offers high reliability and precision, and it is commonly used in airport security and immigration procedures [20].

Facial recognition uses AI and ML algorithms to detect facial features and identify individuals based on their unique characteristics [38]. It is widely used by law-enforcement agencies and at airports. Voice recognition involves analyzing the distinct voice patterns of a person to identify them [39]; it is commonly used in telephone-banking systems and other authenticated services. Behavioral biometrics, on the other hand, tracks human performance patterns such as their typing speed, the way in which they write their signature, their keystroke dynamics, and their mouse movements for identity verification [40]; these approaches are frequently employed in the banking and e-commerce sectors.

Biometric-capture technologies thus offer reliable and secure ways to identify individuals. Each type of biometric technology possesses unique strengths and weaknesses, making each suitable for different applications. The significance of biometrics for enhancing security for safeguarding sensitive data and transactions is evident across various sectors.

Among multiple possibilities, the most commonly used biometric traits in the field of authentication are facial and fingerprint features [41]. Facial recognition stands out as a prominent biometric authentication method due to its non-intrusive nature and the widespread availability of cameras on various devices [3]. AI-based facial-recognition algorithms analyze facial features such as the distance between the eyes, the shape of the nose, and the contour of the jawline to create a unique facial template for each individual. These templates are then used to distinguish and verify identities. Facial recognition is widely used in a variety of sectors to identify and distinguish individuals for security purposes; it is also used on smartphones to securely unlock devices [41–43].

Fingerprint recognition is one of the oldest and most widely used biometric technologies for authentication [1,44]. It involves capturing and analyzing the unique patterns and ridges on a person's fingers to confirm their identity. Fingerprint recognition is highly accurate and has a low FAR, making it a preferred choice in applications that require a high level of security [45]. It is commonly used in smartphones, laptops, and other devices for user authentication, as well as in access-control systems for buildings and sensitive areas [46]. The optimization of fingerprint analysis and classification is crucial for improving the performance of biometric systems, forensic investigations, and other fingerprint-based applications.

The continuous advancement of AI and the integration of biometrics into the IoT is expected to further enhance the capabilities and applications of facial- and fingerprint-recognition technologies, making them even more reliable and secure for various authentication purposes.

4.2. IoT

The IoT is a network of interconnected devices that include embedded sensors, software, and other technologies to collect and exchange data [47]. IoT devices comprise a broad spectrum, ranging from basic sensors to intricate machines or systems. With the proliferation of the IoT, ensuring the security and privacy of these devices has become a significant concern. This section provides an overview of the IoT, IoT security, and IoT authentication.

The IoT has gained immense popularity and is being widely used in various industries, including healthcare, transportation, manufacturing, and smart homes [48]. The use of IoT devices has led to the creation of vast amounts of data, which can be analyzed for insights and to improve efficiencies. However, this also presents challenges for security and privacy [49,50].

IoT security refers to the measures taken to protect IoT devices and networks from cyber threats, such as malware, hacking, and unauthorized access [51]. IoT devices are often vulnerable and can be attacked due to their limited computing resources and weak or default passwords.

Authentication is a fundamental aspect of IoT security, as it ensures that only authorized users and devices can access the network [52]. Authentication is used to verify the identity of users and devices using one or more credentials, such as passwords, tokens, or digital certificates. Authentication helps prevent unauthorized access to devices and IoT networks.

There are several challenges in implementing effective authentication in IoT devices and networks. Authentication mechanisms must be tailored to the specific constraints of IoT devices, such as constrained processing power and memory [53]. The use of strong authentication techniques, such as biometrics, can provide a more secure and convenient alternative to traditional authentication methods [35]. King and Awad [54] proposed a distributed security mechanism that effectively manages and mitigates potential security threats, even in devices with limited processing power, memory, and energy resources. By strategically distributing security tasks and responsibilities, this mechanism optimizes the use of available resources while maintaining a high level of security; through a combination of innovative techniques, such as lightweight cryptography and efficient communication protocols, it aims to protect IoT devices from unauthorized access, data breaches, and other potential cyber threats. This work contributes to the advancement of secure IoT deployment in resource-constrained settings, highlighting the importance of tailored security solutions to safeguard the expanding IoT ecosystem.

In general, the growth of the IoT has created new challenges for security and privacy. IoT security must be addressed to ensure the protection of IoT devices and the data they generate. Authentication plays a crucial role in IoT security and must be implemented effectively to provide secure access control.

4.3. Biometrics for reliable IoT security

Biometric technologies have emerged as a promising solution for improving user security and authentication in IoT devices. By using the unique physiological or behavioral characteristics of individuals, biometrics offers reliable and secure methods to identify and authenticate users and devices in various application domains.

In the era of the IoT, user authentication is crucial to ensuring the security of connected devices. Traditional authentication methods and conventional biometrics-based approaches, such as facial and fingerprint recognition and passwords, are vulnerable to various attacks. However, the powerful sensing capabilities of IoT devices such as smart wearables and smartphones enable the use of behavioral biometrics for continuous authentication. As already noted, behavioral biometrics uses unique patterns of human activity, such as physical movements captured by smartphone sensors, to recognize users [55].

Biometrics in IoT security can be classified into two important categories: authentication and encryption. Yang et al. [8] discussed and classified contemporary biometric-based authentication systems for the IoT based on different biometric traits and the number of biometric traits employed in the system. They also reviewed and discussed biometric-cryptographic systems, which integrate biometrics with cryptography, as a means to enhance security in the IoT. These systems leverage unique characteristics of biometric-capture devices and cryptographic techniques to provide enhanced security for IoT devices [56].

Liao et al. [57] sought to identify the security vulnerabilities, threats, and risks associated with IoT devices and proposed solutions to enhance the security and privacy of IoT systems. Their article discusses various challenges, such as attacks, vulnerabilities, and privacy concerns, and provides information about countermeasures to mitigate these security issues. The results of their literature review provide a comprehensive analysis of security challenges in the IoT and give valuable information about countermeasures to improve IoT security.

The application of biometrics in the IoT extends beyond security. As noted, biometric devices can capture physiological or behavioral features of individuals, and these data can be further processed using cloud computing to verify or identify users [58]. In addition to authentication and security, biometrics can be used for personalized AI services, such as AI secretaries, by analyzing individual speaker data.

Integrating biometrics into IoT systems involves several mechanisms that enable secure and reliable authentication and cryptographic operations. One such mechanism is the use of biometric-capture devices embedded in IoT devices, which capture and process biometric data. These devices can include fingerprint scanners, iris- and facial-capture devices, voice-capturing microphones, and other wearable biometric-capture devices [8].

Dhillon and Kalra [59] addressed the critical demand for robust authentication mechanisms; amid the proliferation of IoT applications, their paper innovatively presents a multi-factor authentication scheme, prominently featuring biometric elements, to increase the security and reliability of remote user authentication. Emphasizing the limitations of conventional methods, the study integrates biometric identifiers such as fingerprints and facial features to enhance user-identification accuracy and bolster trust in the authentication process. Through a meticulously designed framework, which couples biometric factors with passwords or tokens, the scheme establishes a multi-layered security approach to protect against unauthorized access. The outcomes of this research underscore the scheme's effectiveness in fortifying remote-user-access security within IoT settings, propelling advances in securing interactions across the expansive and interconnected IoT landscape.

Biometric-based user authentication is a crucial aspect of IoT security; it ensures that only authorized users can access IoT devices and services [60]. The security of user authentication can be enhanced using biometric traits such as fingerprints, iris patterns, or facial features. Biometric templates are captured during enrollment and compared with the user's biometric data during authentication. This process provides a more secure and more convenient alternative to traditional authentication methods, such as passwords or PINs [61].

Biometric-based cryptography is another mechanism that uses biometrics in IoT systems. This combines the unique biometric traits of individuals with cryptographic algorithms to improve data security and privacy [8]. Biometric-based cryptographic systems use biometric keys derived from a user's biometric traits to encrypt and decrypt data. This ensures that only authorized individuals with the correct biometric traits can access the encrypted data, adding an extra layer of protection [62].

4.3.1. Application domains of biometrics in the IoT

Biometrics has found applications in various IoT domains, including smart homes, industrial automation, transportation, and agriculture. The development of the IoT has paved the way for smart environments, gadgets, and other applications in our daily lives. Biometrics provides security for access control, personalized services, and seamless user experiences in these domains. We will now shed light on two specific application domains: healthcare and smart cities.

- *Healthcare.* In healthcare, biometrics can improve patient identification and the control of access to medical records, enabling secure authentication for healthcare professionals. For example, biometric authentication can be used to ensure that only authorized healthcare providers can access electronic health records, thereby enhancing patient privacy and data security [63,64].
  Biometric security measures such as facial and fingerprint recognition are increasingly being used to ensure patient safety in healthcare organizations. These measures are effective for accurately verifying patient identity, preventing unauthorized access to medical records and hospital data and maintaining the accuracy and safety of patient data [65].
  In the field of healthcare, there have also been studies on the use of iris-recognition systems to detect a person's fitness for duty. These systems can analyze NIR-range iris images to identify changes in iris behavior that may be indicative of impairment due to sleepiness, or alcohol or drug consumption. By detecting such impairments, such systems can help to ensure that individuals are capable of performing their daily tasks safely. This is particularly important in scenarios involving heavy machinery, where impaired individuals can cause work-related accidents and put lives at risk [66,67].
- *Smart cities.* Biometrics plays a vital role in smart-city applications, including for secure access control to smart buildings, intelligent transportation systems, and public safety. Biometric technologies can be employed for efficient and secure identification and authentication in these environments, ensuring that only authorized individuals have access to data, physical facilities, and critical resources and services [48].
  Facilities that use fingerprint-, palm-print-, or facial-recognition technologies can be used to verify the identities of individuals, ensuring authorized access to buildings, transportation systems, and other facilities. Furthermore, digital systems in smart cities can now be equipped with biometrics integrated into payment systems to authorize financial transactions, providing a secure and convenient way for residents to make purchases or access services [26,68].

In summary, the integration of biometrics into the IoT offers exciting opportunities for enhanced security and personalized experiences. Mechanisms such as biometric-based user authentication and biometric-based cryptography can strengthen the security of IoT systems. Additionally, biometric technologies can be applied in various domains, including healthcare and smart cities, enabling secure access control and personalized services.

4.4. AI for robust biometrics

Advanced biometric authentication technologies are increasingly being combined with AI and ML algorithms, leading to enhanced security and privacy for IoT systems. These AI-enabled technologies play a vital role in accurately verifying authorized users and detecting malicious activities within some IoT systems. The integration of AI into biometrics is often referred to as intelligent or AI-powered biometrics [69]. One significant contribution to AI-powered biometric authentication is the use of a combination of multiple biometric features, resulting in multi-layered security. This fusion of multiple biometric traits can be used to provide robust authentication protocols that reduce the risk of errors and decrease FARs [62]. There has also been a growing trend toward AI-powered behavioral biometrics, an approach that provides a more comprehensive solution to biometric authentication. As discussed above, behavioral biometrics analyses user behavior to detect any anomalous activity that may indicate unauthorized access. Unlike traditional biometric approaches that require one-time authentication, AI-based algorithms can continuously monitor user behavior. This technology is currently used in the financial and banking industries to monitor user behavior during online transactions, helping to prevent fraud and illegal activities [18].

The scope of using AI to improve biometric systems is massive, and numerous potential applications have not yet been explored. AI techniques such as ML and DL are playing critical roles in detecting malicious activities in IoT systems. The use of AI will become increasingly vital in biometric authentication mechanisms to combat more sophisticated and increasingly complex cyber threats and attacks, presentation attacks, and software-related attacks [70]. With the widespread adoption of IoT systems, AI in biometric technologies is expected to become more advanced and effective, providing new solutions to the challenges associated with traditional access-control methods [33,71,72].

AI-powered biometric technologies have diverse application potential and have had wide-ranging impacts across multiple industries. Facial- and fingerprint-recognition systems have been increasingly adopted within the security sector, while behavioral biometrics have vast applications in the financial industry, primarily for detecting fraudulent activities. The healthcare and transportation industries have also recently adopted AI in biometric technologies. For example, facial recognition is used in the healthcare industry to identify patients and reduce errors in treatment. As transportation systems become more complex, biometric authentication technologies are being used to identify the drivers of commercial vehicles, and they have also had a positive impact on autonomous-driving applications [33].

From the work reviewed so far, it is apparent that AI-powered biometric technologies have revolutionized traditional authentication mechanisms and provided advanced security and privacy solutions to IoT systems. Authors such as Smith and Miller [73] have addressed crucial ethical considerations related to the deployment of biometric facial-recognition technology. Their study underscored the significance of ethical practices, transparency, privacy protection, and bias mitigation when integrating AI-enhanced facial-recognition systems into biometric applications. Furthermore, the trend toward behavioral biometrics is growing, and the market for behavior biometrics is expected to exceed US $11 billion by 2031 [74]. The scope of AI in biometric technologies is also expected to continue to expand, becoming more advanced and effective with the adoption of increasing numbers of IoT systems, providing unique solutions to the challenges associated with traditional authentication methods.

4.5. The need for AI-powered biometrics in the IoT

The convergence of AI, biometrics, and the IoT has ushered in a new era of enhanced security and personalized experiences. This section focuses on the applications of biometrics in the IoT and the integration of AI and biometrics, with a specific focus on facial and fingerprint recognition.

Integrating biometrics into the IoT opens up novel possibilities for increased security and personalized experiences across various applications. IoT devices, leveraging their interconnected nature and data-gathering capabilities, can derive significant benefits from biometric authentication methods. By incorporating biometric identifiers such as fingerprints, iris patterns, facial features, and voice patterns into IoT systems, seamless and secure user identification can be achieved within the IoT ecosystem [8].

AI has been a game-changer in the field of biometrics, particularly in the fields of facial and fingerprint recognition. AI-driven facial-recognition systems have made substantial strides, enabling accurate and efficient identification of individuals from images or video feeds. These systems use DL algorithms to analyze facial features, such as eye distance, nose shape, and other unique characteristics, to create individualized facial templates [38]. The integration of AI into facial recognition in IoT devices facilitates real-time identification, making it valuable in applications such as access control and surveillance.

Similarly, AI has revolutionized fingerprint recognition. AI algorithms can be used to adeptly extract and analyze minutiae points on fingerprints, which are distinct to each individual, ensuring reliable and secure authentication. The incorporation of AI into fingerprint-recognition systems has substantially improved their accuracy and speed, positioning this as an ideal biometric authentication method for IoT devices [75].

The integration of AI into biometrics for IoT security delivers significant advantages. AI algorithms can continuously learn and adapt from data collected by IoT devices, enhancing the overall performance and accuracy of the recognition of biometric traits. Additionally, AI can empower IoT systems to efficiently analyze and process vast amounts of biometric data, resulting in shorter response times and enhanced user experiences [22].

Furthermore, the integration of AI-powered biometrics into the IoT has ushered in a new level of security and privacy in diverse industries. With real-time data insights from IoT technology, AI algorithms can interpret data to detect suspicious activities within systems. Biometric authentication can ensure precise identification of users, facilitating secure access control. This amalgamation of technologies presents robust and reliable authentication mechanisms [33].

The application of AI-powered biometric authentication to the IoT finds its relevance due to the limitations of traditional authentication methods, which are susceptible to cyber-attacks. Weak passwords have the potential to be easily guessed or brute-forced, and conventional biometrics such as fingerprints and iris recognition carry a higher risk of degraded performance depending on the quality of the provided biometric sample and the performance of the matching module [1,16]. The increased connectivity of IoT devices has also made them prime targets for cybercriminals, necessitating robust authentication mechanisms. The implementation of AI-powered biometrics effectively addresses these limitations [76].

The applications of biometric authentication span various industries. In healthcare, IoT devices are used for patient monitoring, and biometric authentication can be used to secure access to patient data. Many companies in the financial sector have embraced AI-powered biometrics to monitor user behavior during online transactions, mitigating fraudulent activities. In the transportation sector, biometric authentication is used to control vehicle access and secure critical locations. Military and government organizations rely on biometrics for access control to buildings and secure areas [18].

An emerging trend is the adoption of IoT sensors and biometric authentication in smart homes. Sensors in smart homes can collect real-time data, enabling AI algorithms to analyze user behavior and detect anomalies for potential intruder identification. Smart homes implement biometric authentication to ensure authorized access while providing a secure and convenient lifestyle for users [77].

The future scope of deploying AI-powered biometrics in IoT systems is vast. The adoption of IoT-based solutions to provide remote patient monitoring will continue to grow in the healthcare industry, and integrating AI-powered biometrics in IoT systems can provide reliable access control to patient data and improve user privacy. The transportation industry can benefit from more secure vehicle access, leading to improved user experiences. The financial sector is likely to further embrace behavioral biometrics, while military and government organizations can explore DNA technologies as an additional layer of authentication. The implementation of biometrics in smart cities holds the promise of improving urban security while protecting citizens' privacy [77].

In conclusion, the integration of AI and biometrics with applications in the IoT has resulted in enhanced security and privacy, offering advanced solutions to cyber vulnerabilities. The applications of these combined technologies span diverse sectors, from healthcare to smart homes, with a promising future scope. By revolutionizing traditional authentication methods, the implementation of AI-powered biometrics presents a unique opportunity to enhance security and privacy across various industries.

5. Triad of AI, biometrics, and the IoT: A review

The integration of AI, biometrics, and the IoT has emerged as a transformative domain, paving the way for enhanced security, personalized experiences, and a myriad of applications across industries. This convergence brings together the power of AI's intelligent algorithms, the interconnectedness of IoT devices, and the precision of biometric authentication to revolutionize various sectors, addressing the limitations of traditional authentication methods and bolstering security measures.

The integration and deployment of intelligent or AI-powered biometrics in IoT systems offers novel possibilities for securing IoT devices, services, and data. By incorporating biometric authentication methods such as fingerprint and facial recognition, iris scans, and voice recognition into IoT systems, a higher level of security and more seamless user identification can be achieved within the IoT ecosystem [8].

Past trends in this domain have witnessed the continuous development and refinement of AI algorithms, particularly in facial and fingerprint recognition. AI-based facial-recognition systems have evolved significantly, enabling accurate and efficient identification of individuals from images or video feeds. These systems leverage DL algorithms to analyze facial features, creating unique facial templates for each individual [38]. Similarly, AI has made remarkable progress in fingerprint recognition, extracting and analyzing the ridges and points on fingerprints for reliable and secure authentication [75].

In this comprehensive review of the integration of AI and biometrics with applications in the IoT domain, we will delve into past trends, exploring the evolution of AI algorithms and biometric technologies. Furthermore, we will examine current trends and applications, encompassing the healthcare, financial, transportation, and smart home industries. To provide a well-rounded analysis, we will also review various journal papers that contribute to advances in this exciting field. Finally, we will explore the promising future scope, which holds the potential to revolutionize authentication and security measures across industries. Tables 2–7 summarize the reviewed articles in this section.

5.1. Applications of biometrics in the IoT

This section provides a review of existing literature and research on biometric technology and its applications in IoT-based systems, highlighting its significance and potential applications while focusing on security. There are various topics in the field of biometrics, including live face detection, combined iris- and fingerprint-recognition systems, public perceptions of biometrics, the use of biometrics in critical-infrastructure security, the risks associated with biometric technology, data-driven feature-extraction methods, biometric technologies in banking, data privacy protection, and the application of biometrics in body-area networks. Fig. 4 demonstrates the biometric system architecture and its integration with IoT applications. Table 2 and Table 3 summarize the reviewed research related to the applications of biometrics in the IoT.

In 2019, Hamidi [78] proposed an approach to developing a smart health system using the IoT and authentication based on biometric technology. This work sought to improve healthcare services by using IoT devices and biometric authentication. The paper discusses the integration of biometrics and the IoT, emphasizing the role of biometric authentication in ensuring secure and reliable access to healthcare services. The results demonstrate the feasibility and effectiveness of the proposed approach in improving health outcomes.

Splinter [89] studied the realm of eBiometrics, specifically focusing on data acquisition and physiological detection within the context of the IoT. This work aimed to explore the integration of physiological signals, such as heart rate and other vital metrics, as biometric identifiers within IoT-enabled environments. The paper presents a framework for data collection and analysis, emphasizing accurate and real-time physiological sensing. This approach uses IoT-enabled sensors to capture physiological signals, which are then processed and analyzed to establish unique biometric patterns. The results highlight the potential of eBiometrics to contribute to improved identification and authentication mechanisms within IoT systems, enhancing both security and quality of life in smart communities.

Farid et al. [79] present a smart biometric identity-management framework for personalized healthcare services based on the IoT and cloud computing. The work sought to enhance the security and privacy of healthcare services by leveraging biometrics in IoT and cloud-computing environments. The authors propose a framework that combines biometric authentication, data encryption, and access-control mechanisms to protect sensitive healthcare data. The results showcase the potential of the framework to provide secure and personalized healthcare services.

Obaidat et al. [80] discuss the role of biometric security in IoT deployments. Their paper aims to provide an overview of the challenges and advances in biometric authentication for the IoT. It highlights the importance of biometrics in enhancing the security and privacy of IoT systems. The authors discuss various biometric modalities, such as fingerprints, iris patterns, and facial features, and their applications in IoT security. The results emphasize the potential of biometric authentication for providing secure and convenient access control in IoT environments.

In 2021, work carried out by Anand et al. [83] used a pioneering approach to improve security in the realm of 5G-enabled IoT healthcare systems. By seamlessly fusing the power of convolutional neural networks (CNNs) with the precision of biometric authentication, they sought to mitigate concerns surrounding detection of malware attacks (DMA) and unauthorized access to sensitive patient information. The methodology involved the meticulous development of the CNN-DMA model, which is tailored to recognize complex malware patterns within the intricate network dynamics of 5G-IoT healthcare systems. The integration of biometric markers such as fingerprints, retinal scans, and facial recognition enhances the model's ability to quickly detect and counteract potential threats while ensuring a seamless user experience for authorized personnel. While highlighting the model's adaptability and proactive learning mechanisms, the paper also acknowledges its practical limitations, emphasizing the need for real-world implementation and ongoing updates to address evolving malware threats. This innovative fusion of biometrics and DL sets a promising precedent for fortified security and privacy in the expanding landscape of IoT applications, particularly in healthcare settings.

Das et al. [82] provide a noteworthy exploration of the integration of biometrics within the context of the Industrial IoT (IIoT). In

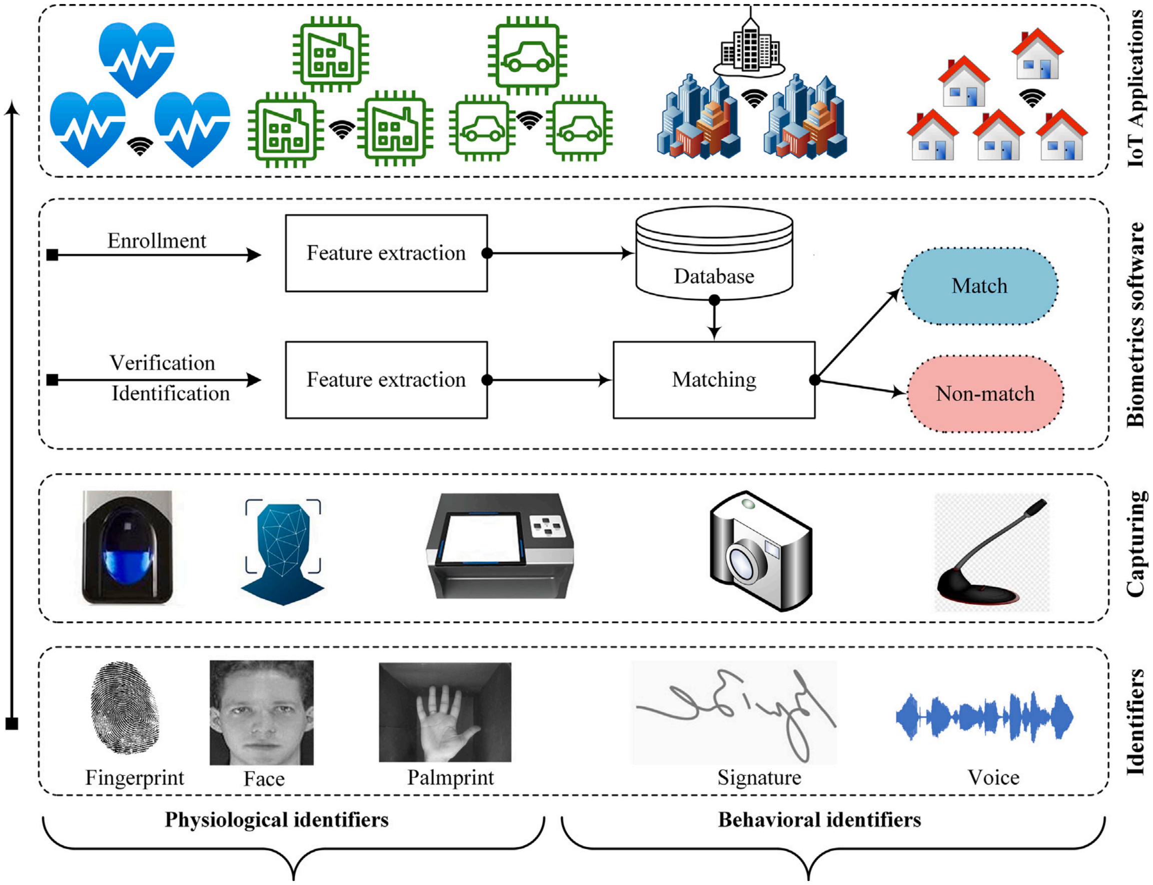

Fig. 4. Biometric system architecture and its integration with IoT applications.

response to the escalating demand for secure and privacy-conscious user-authentication methods in industrial settings, their study introduced an inventive approach. By harnessing biometric attributes such as facial features and fingerprints, the proposed authentication scheme offers a personalized and robust means of user identification. Notably, the paper's distinctive contribution lies in its meticulous attention to privacy preservation. Through the use of advanced encryption techniques and decentralized storage, the scheme ensures that biometric data remain confidential and inaccessible to unauthorized entities. The paper effectively demonstrates the viability of the proposed scheme, presenting a significant advancement in the realm of IoT security. In the broader context of biometrics in IoT, this work serves as a notable stride toward establishing a more secure and trustworthy ecosystem for industrial applications.

Chen et al. [81] present a pioneering approach that leverages radio-frequency (RF) fingerprint identification to enable intelligent mobile edge computing for authentication on the IoT. Their research focused on using unique RF characteristics captured from IoT devices to establish a secure and efficient authentication mechanism. By exploiting distinctive RF fingerprints, the proposed method enhances the authentication process, contributing to improved security and reliability in IoT environments. The study underscores the importance of RF-based authentication in addressing IoT security challenges and highlights its potential impact on securing IoT deployments.

P. Chandel and Kumar [84] explored the integration of IoT technology with fingerprint authentication and genetic-algorithm optimization to mitigate the “black hole” problem, which refers to unauthorized access points in IoT networks. Their paper proposes a novel approach that employs fingerprint biometrics for user authentication, coupled with optimization using genetic algorithms to improve the security of IoT systems. By using genetic algorithms, the system optimizes authentication processes, leading to efficient and robust prevention of black-hole attacks. This research underscores the potential of biometric-based security mechanisms and optimization techniques to bolster IoT security and protect against emerging threats.

Collectively, these papers underscore the objectives, relevance, challenges, and solutions related to IoT security. They stress the importance of tackling security challenges in IoT systems to protect sensitive data, maintain privacy, and prevent unauthorized access. The findings of these studies offer valuable insights into the current state of IoT security research and present potential solutions to enhance the security of IoT devices and networks. These integrations of biometrics into the IoT reveal various advances and possibilities.

Another paper, by Al-Assam et al. [90], addresses the security challenges that emerge in cloud environments, and the authors propose an automated biometric authentication system using cloud computing. They discuss the limitations of traditional security measures and highlight the need for secure data access in cloud environments. The proposed biometric authentication model can be used to enhance security control and mitigate the challenges associated with data access in the cloud.

In 2021, Elordi et al. [91] focused on the deployment of facial-recognition solutions in heterogeneous IoT platforms. Their paper discusses the challenges of deploying DNNs in various IoT devices, and they emphasize the importance of secure management of biometric data while respecting users' privacy. The results of their study highlight the need for appropriate user interaction and optimal deployment strategies for facial-recognition solutions in IoT platforms.

Abosata et al. [85] conducted a comprehensive survey of the integrity of IIoT systems and the existing security approaches for industrial applications. Their review paper discusses the challenges and risks associated with the wider implementation of the IIoT and highlights

Table 2
Summary of reviewed research on the applications of biometrics in the IoT. This table focuses on biometric traits, biometric applications, IoT applications, main contributions, and performance analysis.

Ref.	Biometrics type	Biometric applications	IoT applications	Main contributions	Performance metrics
[9]	Fingerprint	Authentication	General security	Privacy-preserving lightweight biometric system	Authentication speed, privacy preservation, FAR
[43]	Fingerprint, facial	Authentication	Autonomous vehicles industry	Multimodal biometric system using Raspberry Pi	Authentication speed, recognition accuracy, efficiency
[45]	Fingerprint, face, iris, retina	Authentication	General security	Security of biometric authentication systems	Security vulnerabilities, attack vectors, potential risks
[76]	Fingerprint, facial, iris, behavioral	Authentication	Healthcare	Multimodal biometric authentication for personalized healthcare	Recognition accuracy, user acceptance, privacy level
[78]	Various	Authentication	Healthcare	IoT integration for secure healthcare, improved health outcomes	Accuracy, F1 score, feasibility, effectiveness, integration
[79]	Biometric authentication	Authentication	Healthcare	Biometric identity management for personalized healthcare	Accuracy, privacy level, efficiency, potential
[80]	Fingerprint, iris, facial	Authorization	General security	Role of biometrics in IoT security	Recognition accuracy, FAR, potential
[81]	Various	Authentication	General security	Real-time physiological sensing, improved identification	Physiological signal accuracy, real-time processing
[82]	Fingerprint, facial	Authorization	Industrial IoT (IIoT)	Secure and privacy-conscious user authentication	Privacy preservation, user acceptance
[83]	Fingerprint, facial, DNNs	Authentication	Healthcare	Malware detection, biometrics in 5G-enabled healthcare	Malware pattern recognition, user experience
[84]	Fingerprint	Authorization	General security	Genetic-algorithm optimization for IoT security	Prevention of black-hole attacks, efficiency
[85]	Various	Authentication	IIoT	Survey of security approaches for IIoT	Security approaches, integrity of IIoT
[86]	Fingerprint	Authorization	General applications	Security issues and ethical hacking	Security level, vulnerability identification, prevention measures
[87]	Iris	Authentication	General applications	Conceptual view of biometric authentication in the IoT	Integration feasibility, user acceptance, potential benefits
[88]	Facial recognition	Authentication	General security	Privacy-preserving facial recognition framework	Accuracy, confidentiality
[89]	Physiological	Authentication	General applications	Framework for using physiological signals as biometric identifiers	N/A
[90]	Fingerprint, iris, palmprint	Authentication	General applications	Automated biometric authentication systems for cloud environments	Efficiency
[91]	Facial recognition	Authentication	General applications	Secure deployment strategies for DNNs	Real-time processing

the need for security measures. Their results provide insights into the existing security approaches and identify the challenges that arise in ensuring the integrity of IIoT systems.

Ahamed et al. [76] propose an intelligent multimodal biometric authentication model for personalized healthcare services in IoT networks. Their paper emphasizes the growing popularity of biometric authentication in IoT networks and discusses the challenges inherent in providing personalized healthcare services. The results demonstrate the effectiveness of the proposed model in addressing the challenges and enhancing the security of healthcare services.

Fingerprints and facial biometrics are two widely used forms of biometric-capturing technologies in IoT applications. As has been noted throughout this paper, these technologies leverage the unique physical features of individuals for authentication and identification purposes.

Chen et al. [43] propose an IoT-based multimodal biometric authentication system that combines fingerprint and facial recognition. The system uses a Raspberry Pi as the IoT gateway, and this collects biometric data from users. Fingerprints and facial features are extracted and compared with the enrolled templates to authenticate the users. The proposed system was found to achieve high accuracy, and it showed promising results for IoT applications.

Similarly, Yang et al. [9] sought to develop a privacy-preserving lightweight biometric system for IoT security. Their study focused on achieving secure authentication in the IoT while minimizing computational and communication overhead. By leveraging fingerprint biometrics, they address privacy concerns and propose an efficient solution for secure IoT authentication. Yaacoub et al. [86] examined security issues and ethical hacking of IoT devices. Although their paper does not exclusively concentrate on fingerprint biometrics, it provides valuable insights into the broader security landscape of the IoT. Their research emphasizes the need for robust authentication mechanisms, such as fingerprint biometrics, to address the security challenges faced by IoT systems.

The research conducted by Matyáš and Říha [45] investigated the security of biometric authentication systems. While not specifically focused on IoT, their study explored the general security concerns associated with biometric authentication, which can be applied to fingerprint-based authentication in the IoT. By highlighting vulnerabilities and threats, they contribute to an understanding of potential security risks related to deploying fingerprint biometrics in IoT devices. Meena and Choudhary [87] provide a conceptual view of biometric authentication in the IoT. Their paper discusses the application of biometric authentication, including fingerprint-based methods, in IoT systems. By identifying challenges and opportunities, they shed light on the integration of biometrics into the IoT, emphasizing the potential benefits and practical implications of fingerprint biometrics.

Considering facial-recognition-based authentication for IoT applications, Li et al. [88] propose a privacy-preserving facial-recognition framework that is specifically designed for IoT applications. This framework adopts a distributed architecture in which facial features are extracted locally on IoT devices, and the matching process is performed on a secure cloud server. Privacy-protection techniques, such as secure multiparty computation, are employed to ensure the confidentiality of facial data. Their experimental evaluation demonstrates the feasibility and privacy benefits of the proposed framework.

In 2022, the study of Zhang et al. [32] introduced a facial-biometric approach based on DL for secure access control of IoT devices. The proposed method employs a CNN to extract discriminatory facial features, which are then matched against enrolled templates to authenticate users. The system was found to achieve high accuracy and have robustness against various challenges, such as different lighting conditions and pose variations. The experiments the authors conducted validate the effectiveness of DL-based facial biometrics for IoT access control.

Table 3
Summary of reviewed research on biometrics in the IoT. This table focuses on the methodologies, results, and limitations.

Ref.	Methodology	Final results	Limitations
[9]	Proposal and analysis	Privacy-preserving lightweight biometric system for IoT	Limited investigation of potential attacks
[32]	DL-based facial biometric approach	High-accuracy facial recognition for IoT access control	Limited discussion of model interpretability
[43]	System development and evaluation	93%–97% accuracy multimodal biometric authentication system	Limited discussion of computational-resource requirements
[45]	Investigation and analysis	Security concerns and vulnerabilities in biometric systems	Limited exploration of mitigation strategies
[57]	Analysis	Identification of vulnerabilities and security countermeasures	Limited discussion of implementation challenges
[76]	Proposal and evaluation	Intelligent multimodal biometric authentication for IoT healthcare	Limited validation in diverse healthcare scenarios
[78]	Proposal and analysis	Enhanced healthcare services using biometrics with high accessibility	Limited scalability for large healthcare systems
[79]	Framework development	96% accuracy for authentication in personalized healthcare environments	Lack of real-world deployment validation
[80]	Overview and analysis	Enhanced security through biometric authentication in the IoT	Lack of consideration of hardware constraints
[81]	Proposal and analysis	Use of RF fingerprint identification for secure authentication	Limited investigation of RF signal interference
[82]	Innovative authentication scheme	Privacy-preserving authentication with biometric attributes	Limited consideration of usability and user acceptance
[83]	Fusion of CNN and biometric authentication	Detection and prevention of malware attacks in 5G-IoT healthcare	Limited analysis of potential false positives
[84]	Integration of biometrics and genetic algorithms	Prevention of unauthorized access in IoT networks	Limited discussion of computational overhead
[85]	Survey and analysis	Security approaches for integrity of IIoT systems	Limited exploration of emerging IIoT threats
[86]	Analysis and discussion	Need for robust authentication mechanisms in the IoT	Limited coverage of social and ethical aspects
[87]	Discussion and analysis	Challenges and opportunities in biometric authentication in the IoT	Limited focus on standardization efforts
[88]	Proposal and evaluation	Privacy-preserving facial-recognition framework for IoT	Limited consideration of edge-computing resources
[89]	Exploration and framework development	Framework for using physiological signals as biometric identifiers	Limited applicability to non-physiological IoT applications
[90]	Proposal and analysis	Automated biometric authentication system for cloud environments	Limited discussion of potential data leakage
[91]	Analysis and discussion	Optimal deployment strategies for facial recognition in the IoT	Lack of quantitative performance metrics

Table 4
Summary of the reviewed articles on AI-powered biometrics, highlighting biometric traits, AI techniques, and performance metrics.

Ref.	Biometrics type	AI techniques	Performance metrics
[14]	Various biometric modalities	CNN	Accuracy
[92]	Various biometric modalities	SVM, CNN	Correlation matrix
[93]	Fingerprint	CNN	Fingerprint matching accuracy
[94]	EEG sensors	CNN	Identification accuracy
[95]	Invisible ECG	CNN	False-rejection rate, FAR
[96]	Vital signs and stress levels	CNN	Stress-level accuracy
[97]	Facial recognition	CNN	Face-recognition accuracy
[98]	Acoustic characteristics of the outer ear	CNN	Authentication accuracy, equal error rate (EER), FAR
[99]	Heart-rate data	CNN	F1 Score, accuracy, precision, recall
[100]	One-dimensional convolutional models	CNN	Accuracy, F1 score, precision, recall
[101]	Color texture segmentation	CNN	Accuracy, ROC, EER
[102]	Multimodal data fusion	CNN	Accuracy
[103]	Finger vasculature NIR imaging	CNN	NIR imaging accuracy
[104]	Facial expressions	CNN, LSTM, RNN	Accuracy, ROC
[105]	Body channel response	SVM, KNN	Accuracy, EER, ROC
[106]	Fingerprints	CNN, ConvLSTM, ResNet	Accuracy, Predictive positive values
[107]	Facial expressions, poses	CNN	Accuracy

5.2. AI-powered biometrics

This section aims to explore the latest research and advancements in the AI-powered biometrics domain, highlighting the potential of AI-driven biometric authentication systems. Table 4 and Table 5 summarize the reviewed articles on AI-powered biometrics.

One of the main papers delves into the impact of AI and biometric analysis on academic integrity, reversing the engineering of academic honesty [14]; this therefore explores the ethical implications of using AI-driven biometric systems in the context of academic integrity and honesty. The limitations of this study include the focus on a specific domain (academic integrity), which might not fully encompass all ethical considerations related to biometric systems.

In a study conducted by Lancelot Miltgen et al. [92], the acceptance of biometric techniques was evaluated in a voluntary environment. The intention to accept and recommend the technology was measured based on various variables. The study integrated elements from the technology-acceptance model, diffusion of innovations, and the unified theory of acceptance and use of technology to examine the factors

Table 5
Summary of the reviewed research articles based on AI-powered biometrics, highlighting the techniques, results, and limitations.

Ref.	Techniques	Results	Limitations
[14]	CNN	Identified implications for academic integrity due to AI	Focus on a specific domain (academic integrity)
[92]	SVM, CNN	Found factors influencing user acceptance of AI biometric systems	–
[93]	CNN	Achieved improved fingerprint-recognition accuracy with AI techniques	Complexity of the AI model, and computational resources.
[94]	CNN	Developed a method to reduce the EEG sensor count without compromising accuracy and obtained an EER value of 0.0039	Extensive EEG data collection, and individual variations
[95]	CNN	Demonstrated feasibility of continuous monitoring for health and security	Signal-processing challenges and specialized hardware
[96]	CNN	Developed a real-time stress-monitoring wristband system with an accuracy of 76%	Potential privacy concerns related to continuous health monitoring
[97]	CNN	Demonstrated robust facial-recognition system using AI methods	Challenges in real-world implementation
[98]	CNN	Showcased improved authentication accuracy with AI-based techniques and a smaller EER of nearly 0.04	Specialized hardware for acoustic data acquisition
[99]	KNN, MLP, RF, AdaBoost, and LDA	ML model configurations analyzed for stress detection using heart rate and obtained MLP obtained the highest F1 score or 94%	Lack of comprehensive limitations and potential solutions
[100]	CNN	Explored challenges in interpreting features by various CNN models with F1 score range from 0.91 to 0.96	Complexity of model interpretation for DL architectures
[101]	CNN	Achieved robust face anti-spoofing capabilities with an accuracy of nearly 97%	Potential challenges in real-time implementation on FPGA
[102]	SVM, RF, NN	Of the other classifiers, SVM obtained 90% validation accuracy in the gender case and 76.40% for ethnicity	Potential biases in recruitment data and need for diverse datasets
[103]	DNN, ResNet	An average accuracy range from 95% to 100% based on the number of epochs	Potential challenges in image quality and data acquisition
[104]	CNN, LSTM, RNN	Obtained a 97% accuracy for facial emotion-recognition system	Lack of limitations, challenges, and potential solutions
[105]	KNN, SVM	Achieved 95% classification accuracy in AI-based biometric system	Huge amount of data causing imbalance
[106]	CNN, ConvLSTM, ResNet	Achieved average detection accuracy of 97%	Data quality, scalability concerns, and computational-resource restrictions
[107]	CNN	The model achieved an improved accuracy of nearly 80% compared to the initial test results	Data limitation and challenges associated with variations in poses and facial expressions

influencing acceptance. The findings shed light on the determinants of user acceptance of biometrics.

A study by Oblak et al. [93] focused on developing a probabilistic fingermark quality-assessment system using AI techniques. Their methodology involved the analysis of fingermarks and localization of quality regions. The researchers employed AI algorithms to enhance the accuracy of fingerprint recognition and quality assessment. The results demonstrate a significant improvement in fingermark-quality evaluation, contributing to more reliable biometric identification systems. However, the study's limitations lie in the complexity of the AI model and the need for extensive computational resources.

Ortega-Rodríguez et al. [94] present a study aiming to identify the minimum possible number of electroencephalogram (EEG) sensors required for accurate biometric identification. The researchers adopted a data-driven approach and employed AI techniques for feature selection and classification. Their results highlight the potential for reducing the number of EEG sensors while maintaining reliable biometric identification. However, the study's limitations include the need for extensive EEG data collection and individual variations in sensor requirements.

de Melo et al. [95] developed a system-on-chip device for invisible electrocardiography (ECG) biometrics. Their study focused on the integration of AI-based algorithms to process and analyze invisible ECG signals for biometric identification. The results demonstrate the feasibility of continuous and unobtrusive biometric monitoring. However, the limitations of this work lie in the challenges of signal processing and the need for specialized hardware for ECG data acquisition.

In 2023, Mitro et al. [96] presented an AI-enabled smart wristband that offers real-time monitoring of vital signs and stress levels. The researchers employed AI techniques for signal processing and feature extraction from sensor data. The results showcase the accuracy and efficacy of the smart wristband for real-time stress monitoring. However, the study's limitations include potential privacy concerns related to continuous health monitoring.

Saoji et al. [97] propose an attendance-management system using DL and facial-recognition techniques. Their study focused on the development of an AI-based model for accurate and efficient attendance tracking. The results demonstrate high accuracy in facial recognition, enabling seamless attendance management. However, the study's limitations involve potential challenges in real-world implementation, such as lighting conditions and face variations.

Sulavko [98] introduced a novel approach for biometric-based key generation and user authentication using the acoustic characteristics of a person's outer ear. The study employed AI-based correlation neurons to extract and analyze the acoustic features of a person's ear for biometric identification. The results showcase the potential of this unique approach for robust user authentication. However, the study's limitations include the need for specialized hardware for acoustic data acquisition and potential variations in ear characteristics.

The report of Girmay et al. [108] presents an intriguing application of AI in biometrics, focusing on secure and convenient login systems. While the paper outlines the system's design and advantages, it would benefit from offering deeper technical insights, particularly regarding the AI model's architecture and performance metrics. Additionally, a more comprehensive discussion of ethical and privacy concerns related to facial-recognition technology is essential, along with a proposal for regulatory-compliant privacy measures. Evaluating the system's performance through metrics such as accuracy, FAR, and false-rejection rate (FRR) would provide valuable insights.

The study carried out by Aquino et al. [100] in 2022 focused on explaining one-dimensional convolutional models in human-activity recognition and biometric-identification tasks. The study employed AI techniques for model interpretation and feature visualization. The results offer valuable insights into the discriminatory features learned by convolutional models. However, the limitations lie in the complexity of model interpretation for DL architectures.

Moon et al. [101] propose a face antispoofing method using color/texture segmentation on a field-programmable gate array (FPGA). Their study employed AI techniques for color and texture segmentation and face-liveness detection. The results demonstrate effective face-antispoofing capabilities. However, the study's limitations include potential challenges in real-time implementation on FPGA devices.

Peña et al. [102] present recent advances in human-centric multimodal ML and its application in AI-based recruitment. Their study employed AI techniques for multimodal data fusion and the development of ML models. The results showcase the potential of multimodal ML to improve recruitment processes. However, the limitations involve potential biases in recruitment data and the need for diverse datasets.

Fiolka et al. [103] propose a multi-wavelength biometric-acquisition system using NIR imaging of the finger vasculature. Their study employed AI techniques for image analysis and feature extraction from finger-vasculature images. The results demonstrate the feasibility of using NIR imaging for biometric identification. However, the limitations lie in potential challenges relating to image quality and data acquisition.

The work done by Rodriguez et al. [104] focused on enhancing the accuracy of facial-expression classification using long short-term memory (LSTM) networks within the realm of AI-based biometrics. Their study sought to advance the comprehension and recognition of human emotions by developing a computational model named "Deep Pain". Employing DL techniques and LSTM networks, the researchers processed and analyzed facial images to achieve improved accuracy in identifying facial expressions. Notably, the proposed Deep Pain model was found to achieve a remarkable accuracy rate of 97% in facial emotion recognition, highlighting the efficacy of LSTM networks in enhancing the state-of-the-art performance in this domain. However, this work could benefit from a more comprehensive exploration of potential limitations, challenges, biases, and the practical implications associated with the deployment of the model; this would offer a more comprehensive understanding of its capabilities and limitations.

The research conducted by Kang et al. [105] aimed to explore the viability of using the human body's channel response as a distinctive biometric trait for recognition purposes. Through a series of experiments, they investigated the electrical characteristics of the human body and the potential for this to be used for biometric authentication. The authors meticulously measured and analyzed the human body's channel response under various conditions, considering factors such as posture and measurement locations. Their results revealed unique patterns in the human body's channel response that could be used to differentiate individuals. However, the authors acknowledge limitations, such as potential variability due to external factors, the complexity of measurement setups, ethical concerns, and the need for broader generalization. Despite these limitations, the research sheds light on the potential of using the human body's channel response as a novel biometric feature, contributing to the exploration of innovative AI approaches in the field of biometric recognition.

The study of Sedik et al. [106] focused on the use of advanced AI techniques to enhance the security of biometric identification systems within the framework of smart cities enabled by 5G. By addressing the security challenges inherent in urban environments, the study aimed to detect unauthorized alterations in biometric data by developing and evaluating DL models. Through the use of diverse DL architectures, including CNNs and RNNs, the results demonstrated the efficacy of these modalities for accurately identifying irregularities in generated biometric information. Although it sheds light on the potential for AI-driven alteration detection, the paper also acknowledges potential limitations, such as data-quality dependencies, real-world scalability concerns, and computational-resource requirements. It nonetheless contributes valuable insights toward bolstering the integrity of identity-verification processes in modern urban landscapes.

Wang et al. [107] focused on the development of a facial-recognition system that harnesses the capabilities of CNNs, which are renowned for their effectiveness in computer-vision tasks, particularly facial recognition. The methodology for the proposed system is anticipated to involve the design of the architecture of the CNN model, examination of the intricacies of its training procedures, and consideration of data-preprocessing techniques. Moreover, it is expected to yield results that include an evaluation of the system's performance metrics, such as accuracy and efficiency. Nevertheless, it is essential to recognize that specific paper details are not provided here. The study may also entail limitations, such as addressing the challenges associated with variations in lighting conditions, poses, and facial expressions.

The field of AI in biometrics is rapidly progressing, holding significant potential to revolutionize information and data security, privacy, healthcare, and other domains. The studies highlighted in this review demonstrate how AI techniques, particularly DL, can effectively enhance the accuracy and efficiency of biometric systems, including capturing devices. As AI technology continues to advance, we can expect more innovative applications and improved security standards in biometrics. Together, these studies contribute to the growth of knowledge in the field, driving advances in secure IoT deployments through the integration of biometrics and AI. Nonetheless, further research is necessary to address ethical implications and user acceptance and ensure the resilience of AI-driven biometric systems against emerging threats.

5.3. AI-powered biometrics for the IoT

In recent years, researchers have been actively exploring the application of AI in the fields of biometrics and the IoT. Several articles have contributed to our understanding of the role of AI-powered biometrics in the IoT domain, with a strong emphasis on its effectiveness in enhancing security and authentication. Table 6 and Table 7 summarize the reviewed articles on AI-powered biometrics for the IoT.

Biometric systems can be evaluated using different metrics to gauge their accuracy, reliability, and overall effectiveness depending on an adjusted threshold. These metrics include FAR, FRR, and equal error rate (EER). The FAR measures the likelihood of the system accepting an unauthorized individual or imposter incorrectly. A lower FAR indicates a more secure system. The FRR measures the likelihood of the system incorrectly rejecting genuine users. A lower FRR indicates better convenience for users. Finally, the EER represents the point at which the FAR and FRR are equal, which provides a balanced assessment of the performance of a biometric system [115,116]. These evaluation parameters are relevant to Table 7.

The study published in 2020 by Liang et al. [33] sought to explore the integration of behavioral biometrics as a mechanism for continuous authentication within the IoT landscape, leveraging the capabilities of AI techniques. In the paper, the researchers explore the potential of harnessing behavioral traits, such as keystroke dynamics and

Table 6

Summary of AI-powered biometrics in IoT systems. This table focuses on AI algorithms, biometric technologies, and IoT layers.

Ref.	Type of biometrics	Biometric applications	IoT layer	AI algorithms
[15]	Behavioral	Authentication	Application layer	HD-sEMG
[32]	Face, fingerprint, iris, and others	Authentication and authorization	Application layer	CNN, DBN
[33]	Behavioral biometrics	Authentication and authorization	Application layer	SVM, CNN, LSTM, GAN
[55]	Behavioral biometrics	Authorization	Application layer	CNN, bidirectional LSTM
[58]	Iris, facial recognition	Authentication	Application layer	Logistic regression, GAN
[109]	Facial biometrics	Authentication	Device layer	LBPH
[110]	Facial recognition	Authorization	Application layer	Haar cascade classifier, LBPH
[111]	Voice biometrics	Authentication and authorization	Application layer	STD, statistical models
[112]	Facial recognition	Authentication	Application layer	MTCNN
[113]	Machine biometrics	Authorization	Device layer	MLP, LSVC, DT, KNN, LR, RF, SGD, XGB, XGBRF
[114]	Fingerprint, face	Authentication	Application layer	RBM, CNN, VGG-16 Net

Table 7

Summary of the literature on AI-powered biometrics deployed in IoT systems. This table focuses on the aims, methodologies, results, and limitations.

Ref.	Aim	Methodology	Performance metrics	Results	Limitations
[15]	Develop gesture-based authentication using HD-sEMG for IoT security	Novel authentication using HD-sEMG and AI, emphasize gesture-based authentication	EER	Potential of HD-sEMG for IoT security with low EER values less than 0.05	Practicality and user acceptance
[32]	Explore AI-based physiological-characteristic recognition for IoT authentication	Use AI to analyze physiological signals for user authentication	Accuracy, recall, EER, verification rate	Potential of AI in improving IoT authentication	Execution capability of the devices must also be considered
[33]	Explore behavioral biometrics for continuous IoT authentication using AI	Integration of behavioral traits (keystroke dynamics, touch patterns) for dynamic authentication	Accuracy, EER	Successful application of AI-driven behavioral biometrics	Variations in behavioral patterns, user acceptance challenges
[55]	Develop continuous user authentication on mobile devices using AI	Creation of time-series dataset for continuous user authentication	Accuracy, FAR	Efficacy of continuous mobile-user authentication with 98.4% accuracy	Need for diverse datasets
[109]	Design a real-time door-unlocking system using facial biometrics and IoT	Integration of facial-recognition technology with IoT architecture for door access control	Confidence rate	Successful implementation of real-time door-unlocking system with 88% confidence rate	Accuracy in varying lighting conditions, system optimization
[110]	Propose IoT-based mobile surveillance robot with facial recognition	Development of IoT-based mobile robot with face recognition for surveillance	ROC, accuracy	Successful integration of the IoT and facial recognition with CNN that gives the highest accuracy of 93.33%	Lack of specific evaluation results
[111]	Investigate trust and voice biometric authentication for IoT	Study trust establishment using voice biometrics for IoT users	Mean, median, SD, p value	Potential benefits of voice-based authentication with 0.86 p value	User acceptance, robustness against voice mimicry
[113]	Introduce "machine biometrics" for identifying machines in smart cities	Explore unique identification and authentication of machines using AI	Accuracy, precision, recall, F1-score	Successful machine identification with 98% accuracy	Challenges in handling diverse machines, scalability, privacy concerns
[114]	To develop a robust intrusion-detection system for a smart city using biometric authentication and AI-driven IoT devices	Integration of AI algorithms to analyze biometric data and device network patterns, deployment of IoT sensors for real-time biometric data collection	Detection accuracy, FAR, FRR, response time	Achieved a detection accuracy of 95%, with an FAR of 3% and an FRR of 2%	Limited diversity, privacy, and scalability

touch patterns, to establish a seamless and dynamic authentication process. It presents new perspective on enhancing security through AI-powered behavioral biometrics, contributing to the evolving paradigm of continuous and unobtrusive authentication in the IoT era. The methodology involves collecting and analyzing user-specific behavioral features, which are then employed to build AI models that are capable of distinguishing authorized users from potential intruders. The results highlight the efficacy of this approach in enabling continuous authentication and bolstering IoT security. However, the limitations of this work include potential variations in behavioral patterns due to contextual factors and user-acceptance challenges associated with unobtrusive authentication methods.

Recently, Krishna et al. [109] presented an innovative real-time door-unlocking system that capitalizes on the synergy of facial biometrics and IoT. The aim of the study was to design a secure and efficient mechanism for door access control, integrating facial-recognition technology into an IoT architecture. The system description involves the setup of a door-lock system equipped with IoT sensors and actuators capable of responding to real-time facial-recognition processes. The methodology encompasses the development of a facial-recognition algorithm and IoT protocols for seamless interaction between the biometric authentication process and the door-locking mechanism. The results indicate a successful implementation of this real-time door unlocking system, highlighting the potential for enhanced security and convenience in access-control scenarios. However, limitations of the work include challenges related to the accuracy of facial recognition in varying lighting conditions and the need for continuous system optimization for robust performance.

Jiang et al. [15] present a novel approach using cancelable high-density surface electromyography (HD-sEMG) for biometric authentication, highlighting gesture-based authentication as a means to improve IoT device security. The limitations of their research include the practicality and user acceptance of using gesture-based authentication in real-world IoT scenarios using AI applications. Some researchers have criticized proposed biometric authentication schemes. For example, Hussain and Chaudhry [11] raised concerns about the privacy-preserving user-authentication scheme for cloud-based IoT deployment, pointing out potential vulnerabilities.

However, the report of Meddeb et al. [110] proposes a cost-effective prototype mobile surveillance robot based on the IoT, which can be seamlessly integrated into industrial areas. This intelligent robot employs the IoT and facial-recognition technology to enhance safety through real-time facial-recognition processing. Equipped with a passive infrared sensor and camera, the robot captures live-streaming videos and photographs that are transmitted to a control room via the IoT. The facial-recognition algorithms, namely a Haar cascade classifier (HCC) and local binary pattern histogram (LBPH), enable the system to distinguish between authorized personnel and potential intruders. When an unauthorized individual is detected, the system triggers alert notifications and sends an email with the captured image to the control room. The authors have developed a web interface for remote control of the robot using Wi-Fi connectivity, facilitating efficient monitoring of a wide area. The paper describes the system's development, the integration of AI and IoT technologies, and the use of facial-recognition algorithms. It emphasizes the practicality and potential of the proposed approach for enhancing surveillance systems. However, the paper does not present specific results from these evaluations, leaving room for future performance assessments.

Wells and Usman [111] investigated trust and voice biometrics authentication for the IoT, aiming to establish secure and trusted authentication methods. Their report covered voice biometrics and its potential to establish trust for IoT users. The results demonstrate the potential benefits of combining voice-based authentication with trust mechanisms. However, the limitations of the work include the need for user acceptance and robustness against voice-mimicry attacks.

Jaswal et al. [112] discuss an AI-driven smartphone app for post-COVID home-quarantine management, showcasing the application of AI in biometrics for authentication purposes. The system uses AI techniques, including biometric facial recognition, to ensure strict home-quarantine management, enhancing the accuracy and reliability of biometric authentication systems for effective monitoring and control.

Another relevant paper, reporting a study conducted by Huang et al. [58], focuses on the application of biometrics in personalized AI services within IoT environments. The authors highlight how biometric sensors can capture physiological or behavioral features that can be processed using cloud computing to verify or identify users. They discuss the potential of biometrics for enabling personalized AI services such as AI secretaries and enhanced authentication, expanding the scope of biometrics and its role in facilitating personalized AI experiences in the context of the IoT.

The report published in 2021 by Sidiropoulos and Papakostas [113] investigates the novel concept of "machine biometrics" within the context of a smart-city environment. The aim of the study was to explore innovative ways to uniquely identify and authenticate machines in the burgeoning landscape of the IoT, thereby enhancing the operational efficiency and security of smart-city systems. The authors provide a comprehensive description of their proposed methodology, which involves the integration of AI techniques into biometric principles to create distinct and reliable "biometric" signatures for machines. These signatures, which are derived from various machine-specific characteristics and behaviors, enable accurate identification and tracking of machines in real time. The paper showcases their results by demonstrating the successful application of machine biometrics in a smart-city setting, where machines are accurately identified, authenticated, and monitored to facilitate seamless IoT operations. However, like any pioneering research, this study acknowledges its limitations, such as potential challenges in handling diverse types of machines, ensuring scalability, and addressing potential privacy concerns.

Recently, Alzahrani et al. [55] aimed to develop an innovative system for continuous user authentication on mobile devices. Their methodology involves collecting behavioral biometric data, including touch gestures and interaction patterns, to create a time-series dataset. The proposed approach combines a CNN for spatial-feature extraction and a bidirectional LSTM model to capture sequential dependencies in the data. The hybrid model was trained and validated on a labeled dataset that contained genuine user interactions and potential impostor attempts. The obtained results demonstrate the system's efficacy in achieving high accuracy and low FARs, enhancing the security of mobile devices. However, potential limitations and the need for diverse datasets are also discussed. This research contributes to the advancement of continuous mobile-user authentication techniques, leveraging the power of DL to provide secure and seamless authentication experiences.

In their 2022 paper, Zhang et al. [32] explore the application of AI in physiological-characteristic recognition for IoT authentication. The authors discuss the use of AI algorithms to analyze physiological signals, such as heart rate and gait patterns, for user authentication in IoT systems. By leveraging AI techniques, this biometric authentication system becomes more robust and resistant to spoofing attacks, highlighting the potential of AI for improving the security and reliability of biometric authentication in IoT scenarios.

The report of Annadurai et al. [114] presents a comprehensive study at the intersection of biometric authentication, AI, and the IoT, aiming to establish an advanced intrusion-detection system within a smart-city environment. By amalgamating biometric data collection, the use of AI algorithms for analysis, and strategic deployment of IoT sensors, the approach achieves a robust security framework. A performance evaluation of the system demonstrates a high detection accuracy of 95%. However, the paper acknowledges limitations such as potential diversity gaps in biometric data representation, privacy concerns in the handling of biometric information, and scalability challenges in larger smart-city implementations. Overall, the paper underscores the potential of the amalgamation of biometrics, AI, and the IoT for enhancing smart-city security while acknowledging avenues for future improvements.

In summary, the reviewed papers provide valuable insights into the role of biometric technology in the IoT and highlight relevant research in AI-powered biometrics. They cover various aspects such as behavioral biometrics, AI algorithms, authentication systems, cryptographic techniques, and personalized AI services, significantly improving our understanding of the potential applications, challenges, and advances in leveraging biometrics to enhance security and authentication in IoT systems.

6. Open challenges and future vision

The integration of the triad of AI, the IoT, and biometrics has great potential for various applications and industries. However, there are several open challenges that need to be addressed to fully realize the benefits of this integration and shape its future directions.

6.1. Challenges in AI-powered biometrics for the IoT

The challenges in this field can be summarized as follows.

- *Cross-device authentication.* Recently, increasing numbers of people are becoming multi-device users, interacting with multiple smart devices [33]. The complexity of multi-device, multi-user interaction presents significant challenges for cross-device authentication. Previously, research has assumed a one-to-one mapping between a user and a device, and it has mainly focused on user authentication in a single-device scenario. However, now, the relationships between users and devices in multi-user, multi-device scenarios are becoming many-to-many. Thus, transferring a pretrained user-identification model from a source domain to a target domain has rarely been studied. Hintze et al. [117] propose a multimodal and cross-device authentication system based on behavioral and physiological biometrics (e.g., gait, voice, face, and keystroke dynamics) to reduce the manual burden of user verification according to the context such as location, time of day, and nearby devices.

- *Emerging malicious attacks on biometrics-based authentication.* Most authentication systems based on behavioral biometrics are prototypes evaluated in a constrained laboratory environment with limited numbers of participants. Comprehensive evaluations with large numbers of participants are needed to investigate the performance of existing behavior-based authentication systems when they are faced with potential attacks. Moreover, IoT systems are faced with numerous security threats in the physical, protocol, communication, and application layers [118]. For example, in a low-power wireless network, an energy-depletion attack can rapidly drain the batteries of devices by forcing sensors or actuators to execute energy-intensive tasks. Consequently, an entire network could fail due to battery exhaustion [119]. Thermal attacks rely on the heat transferred from users to interactive devices and exploit heat traces in the wake of user interaction with devices to uncover the entered credentials [120]. In the communication layer, heterogeneous communication protocols are subject to attacks such as eavesdropping, sinkhole, hello flood, and collision [121]. AI is widely applied by imposters to hack authentication and identification systems. For example, AI has been maliciously used by imposters to speculate passwords [33].
- *Security and privacy challenges.* Biometric authentication systems face challenges such as spoofing attacks, template protection, and secure storage of biometric data [10,17,24,26]. Privacy concerns arise when personal biometric data is collected and processed in IoT environments [8,20]. Striking a balance between usability and privacy is crucial [42]. To overcome these challenges, privacy-preserving mechanisms and regulatory frameworks should be used to safeguard user data and privacy.
- *Usability and user experience.* Combinations of biometric systems with AI and the IoT should strive for higher accuracy and efficiency [8,14,21]. Improving algorithms and leveraging AI techniques can enhance recognition rates and reduce FARs and FRRs. In addition, user experience is crucial for a widespread adoption and the move toward seamless integration and a user-friendly interface. The development of intuitive interfaces and the seamless integration of biometric authentication in IoT-based devices and IoT applications can overcome these challenges [14,25].
- *Ethical and legal considerations.* The collection, storage, and use of biometric data raise ethical concerns [9,24]. Ensuring data privacy and adhering to ethical frameworks can help to ensure the responsible use of biometric data and minimize potential biases and discriminatory practices. Furthermore, adhering to legal regulations is crucial for the integration of AI, the IoT, and biometrics [20]. During the development of such systems, compliance with existing and emerging data-protection and privacy laws is essential to ensuring transparency and accountability.
- *Interoperability and standardization.* The integration of AI-powered biometrics into the IoT requires interoperability among different systems, devices, and platforms [11,22]. This includes the development and application of standardized protocols and frameworks to ensure seamless integration and communication between various IoT and biometric systems. Additionally, standardization plays a vital role in ensuring compatibility, security, and reliability [17].

6.2. Future vision

The process of the integration of AI into biometrics produces AI-powered biometric systems that can be applied to enhance IoT security. This holds significant promise for the future, with numerous advances and trends anticipated in various industries and applications. As an outcome of the review process, we have identified the following future trends in the application of AI-powered biometrics to the IoT.

- *AI-powered biometric systems.* Leveraging DL algorithms to extract high-level features from biometric data will lead to improved accuracy and recognition rates [8,14,21]. Explainable AI plays a crucial role in biometrics, enhancing transparency and trust in AI-driven systems [122]. By developing explainable AI models, it is possible to gain insights into how biometric algorithms make decisions based on physiological or behavioral features, providing clear justifications for outcomes. This transparency is vital in critical applications such as authentication and identification, where users need to understand the reasoning behind AI decisions. Furthermore, using explainable AI helps to identify biases and ethical concerns, promoting fairness and ethical use of biometric technologies [55].

  Striking a balance between model complexity and interpretability remains a challenge, especially in complex AI models such as those using DL [123]. Nonetheless, pursuing interpretability in biometrics fosters greater acceptance and ensures that AI-powered biometric systems deliver reliable and trustworthy results in various domains. Continued research in explainable AI will unlock the full potential of biometrics while addressing concerns and promoting ethical deployments of AI technologies.
- *ML advances.* So-called “Tiny ML” is the future. This involves deploying ML models on resource-constrained IoT devices, and it is poised to play a significant role in this context. With advances in hardware and software optimization techniques, Tiny ML is expected to become even more efficient, accurate, and accessible in the future [124]. This will open up new possibilities for applications such as predictive maintenance in smart homes, health monitoring in wearable devices, and real-time environmental monitoring.

  Another technology that is currently emerging is automated ML (AutoML) applications. As the volume of data grows exponentially, the complexity of ML models and hyperparameter tuning will increase, necessitating advanced automated solutions. AutoML, which automates the ML workflow, is expected to remain a powerful tool in the future of AI and ML. It will continue to democratize AI by enabling more people to harness the power of ML without the need for extensive expertise [125].

  In various domains, including healthcare, financial services, autonomous vehicles, and climate science, AutoML is anticipated to assist in developing sophisticated models and optimizing complex tasks. As the field evolves, AutoML techniques are likely to become more sophisticated, addressing complex challenges and reducing the need for extensive human intervention in the model-development process.
- *Advances in biometric security.* Continuous monitoring and verification of a user’s identity based on unique biometric traits will enhance security and mitigate the risks of unauthorized access [10,17,24,26]. Furthermore, integrating multiple biometric mechanisms, such as fingerprints, facial recognition, and voice recognition, will result in more robust and accurate authentication systems; however, such systems should not compromise usability, and the implementation of such multimodal systems should only be used if required by the desired level of security [10,79].
- *IoT-driven biometric applications.* Integrations of AI, biometrics, and the IoT will revolutionize a variety of applications. For instance, healthcare services can be improved through the implementation of IoT systems for personalized and remote patient monitoring, early detection of diseases, and customized treatment plans. Adding biometrics to IoT devices will create a strong security layer, which will increase the trust and user acceptability of the services offered [114]. In smart homes and cities, adding biometric-capture devices will enhance security and convenience, enabling seamless access control, personalized services, and efficient resource management [49,112]. Future focus will be on the development of techniques such as secure encryption, federated learning, and differential privacy to protect user data while maintaining acceptable usability [8,20].

- *Standardization and interoperability.* Endeavors toward standardization will establish common frameworks, protocols, and data formats, ensuring seamless integration and communication among AI, biometrics, and IoT systems [11,22]. Other advances that emerge from AI-powered biometrics and the IoT include wearable electronics and photonics, real-time healthcare monitoring, incorporation of behavioral biometrics into IoT devices for continuous authentication, AI-enabled threat detection and response, automated civil infrastructure, health monitoring, and intelligent energy management in smart grids [11,12,55,126–129].

  The deployment of IoT system has the potential to have positive impacts on various sectors, including healthcare, infrastructure monitoring, energy management, and smart cities. However, challenges regarding security, privacy, interoperability, and ethics need to be addressed, and AI-powered biometrics will play a vital role to this end. Overcoming these challenges has the potential to result in significant improvements in efficiency, security, privacy, safety, and quality of life.

  There are new trends and advances in biometric technology that enhance healthcare security. These include multi-factor authentication, which uses multiple biometric modalities such as fingerprint scans and facial recognition. Another advance in this area is continuous authentication which, a noted, is a real-time monitoring and identity-verification approach that can offer alerts relating to threats or unauthorized access to sensitive information. Finally, biometric-enabled applications can be applied to apps, in-home devices, and other technologies to provide better and more secure access to patient records.

It is important to note that the challenges identified herein and the future vision presented above provide opportunities for further research aimed at either overcoming these challenges or advancing the application of AI-powered biometrics in the IoT.

7. Conclusion

The IoT has great potential in various applications, such as autonomous vehicles, healthcare, industry 4.0, and smart cities. However, due to the size and diversity of the data and applications, this will require intelligent and scalable security measures. Integrating AI into biometric technologies such as fingerprint and facial recognition creates intelligent or AI-powered biometric systems, and this in turn contributes to developing security solutions that meet IoT security requirements. In this article, we have presented a comprehensive review examining the current literature on biometrics, intelligent or AI-powered biometrics, and the IoT, focusing on different aspects and challenges associated with this integration, as well as envisioning future trends.

This review has highlighted the important role of biometrics in enhancing IoT-based system security, emphasizing the need for intelligent biometrics that use AI to create AI-powered biometric-based security measures that are suitable for the IoT. The review has also discussed exciting possibilities, such as the convergence of AI, biometrics, and the IoT, the use of enhanced biometrics in IoT domains, and the interdependence of these three components.

Although there are challenges to be addressed, such as security and privacy concerns, the lack of resources in IoT devices, cross-device authentication, security attacks on AI, authentication and encryption, and ethical issues, this integration has the potential to transform future innovations. Future investigations are required to address the identified challenges. By addressing these challenges, the full potential of this triad can be realized, leading to an intelligent, secure, and interconnected future that will positively impact many aspects of human life.

CRediT authorship contribution statement

Ali Ismail Awad: Conceptualization, Investigation, Methodology, Project administration, Visualization, Writing – original draft, Writing – review & editing. **Aiswarya Babu:** Data curation, Investigation, Methodology, Visualization, Writing – original draft, Writing – review & editing. **Ezedin Barka:** Investigation, Writing – original draft, Writing – review & editing. **Khaled Shuaib:** Investigation, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

We would like to express our sincere gratitude to the anonymous reviewers for their valuable feedback and suggestions, which have improved the quality of this work. This work was supported by a joint research grant between United Arab Emirates University and Zayed University (UAEU-ZU), under the Big Data Analytics Center at UAEU, United Arab Emirates (Grant No. 12R141).

References

[1] Maltoni D, Maio D, Jain AK, Prabhakar S, et al. Handbook of fingerprint recognition. Vol. 2, Springer; 2009.

[2] Unar J, Seng WC, Abbasi A. A review of biometric technology along with trends and prospects. Pattern Recognit 2014;47(8):2673–88. http://dx.doi.org/10.1016/j.patcog.2014.01.016.

[3] Jain AK, Nandakumar K, Ross A. 50 Years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognit Lett 2016;79:80–105. http://dx.doi.org/10.1016/j.patrec.2015.12.013.

[4] Mamdouh M, Awad AI, Khalaf AA, Hamed HF. Authentication and identity management of IoHT devices: Achievements, challenges, and future directions. Comput Secur 2021;111:102491. http://dx.doi.org/10.1016/j.cose.2021.102491.

[5] Elrawy MF, Awad AI, Hamed HF. Intrusion detection systems for IoT-based smart environments: a survey. J Cloud Comput 2018;7(1):1–20.

[6] Awad AI, Abawajy J. Security and privacy in the Internet of things: Architectures, techniques, and applications. John Wiley & Sons; 2021.

[7] Alani MM, Awad AI, Barka E. ARP-PROBE: An ARP spoofing detector for Internet of Things networks using explainable deep learning. Internet Things 2023;23:100861. http://dx.doi.org/10.1016/j.iot.2023.100861.

[8] Yang W, Wang S, Sahri NM, Karie NM, Ahmed M, Valli C. Biometrics for internet-of-things security: A review. Sensors 2021;21(18):1–26. http://dx.doi.org/10.3390/s21186163.

[9] Yang W, Wang S, Zheng G, Yang J, Valli C. A privacy-preserving lightweight biometric system for internet of things security. IEEE Commun Mag 2019;57(3):84–9. http://dx.doi.org/10.1109/MCOM.2019.1800378.

[10] Dass SC, Zhu Y, Jain AK. Validating a biometric authentication system: Sample size requirements. IEEE Trans Pattern Anal Mach Intell 2006;28(12):1902–13. http://dx.doi.org/10.1109/TPAMI.2006.255.

[11] Hussain S, Chaudhry SA. Comments on 'biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment'. IEEE Internet Things J 2019;6(6):10936–40. http://dx.doi.org/10.1109/JIOT.2019.2934947.

[12] Sodhro AH, Awad AI, van de Beek J, Nikolakopoulos G. Intelligent authentication of 5G healthcare devices: A survey. Internet Things 2022;20:100610. http://dx.doi.org/10.1016/j.iot.2022.100610.

[13] Hussain A, Khan SU, Khan N, Shabaz M, Baik SW. AI-driven behavior biometrics framework for robust human activity recognition in surveillance systems. Eng Appl Artif Intell 2024;127:107218. http://dx.doi.org/10.1016/j.engappai.2023.107218.

[14] Oravec JA. AI, biometric analysis, and emerging cheating detection systems: The engineering of academic integrity? Educ Policy Anal Arch 2022;30. http://dx.doi.org/10.14507/EPAA.30.5765.

[15] Jiang X, Liu X, Fan J, Ye X, Dai C, Clancy EA, et al. Enhancing IoT security via cancelable HD-sEMG-based biometric authentication password, encoded by gesture. IEEE Internet Things J 2021;8(22):16535–47. http://dx.doi.org/10.1109/JIOT.2021.3074952.

[16] Jain A, Flynn P, Ross A. Handbook of biometrics. Springer US; 2007.

[17] Tomicic I, Grd P, Baca M. A review of soft biometrics for IoT. In: 2018 41st international convention on information and communication technology, electronics and microelectronics, MIPRO 2018 - proceedings. Croatian Society MIPRO; 2018, p. 1115–20. http://dx.doi.org/10.23919/MIPRO.2018.8400203.

[18] Gayathri M, Malathy C, Prabhakaran M. A review on various biometric techniques, its features, methods, security issues and application areas. In: Advances in intelligent systems and computing, vol. 1108 AISC, 2020, p. 931–41. http://dx.doi.org/10.1007/978-3-030-37218-7_99.

[19] Junaid SB, Imam AA, Shuaibu AN, Basri S, Kumar G, Surakat YA, et al. Artificial intelligence, sensors and vital health signs: A review. Appl Sci (Switzerland) 2022;12(22):1–25. http://dx.doi.org/10.3390/app122211475.

[20] Khoirunnisaa AZ, Hakim L, Wibawa AD. The biometrics system based on iris image processing: A review. In: Proceedings - 2019 2nd international conference of computer and informatics engineering: artificial intelligence roles in industrial revolution 4.0. (December):2019, p. 164–9. http://dx.doi.org/10.1109/IC2IE47452.2019.8940832.

[21] Xue Q, Ju X, Zhu H, Zhu H, Li F, Zheng X. A biometric-based IoT device identity authentication scheme. In: Lecture notes of the institute for computer sciences, social-informatics and telecommunications engineering, LNICST, vol. 287, Springer International Publishing; 2019, p. 139–49. http://dx.doi.org/10.1007/978-3-030-22971-9_12.

[22] Kumar NM, Chand AA, Malvoni M, Prasad KA, Mamun KA, Islam FR, et al. Distributed energy resources and the application of AI, IoT, and blockchain in smart grids. Energies 2020;13(21). http://dx.doi.org/10.3390/en13215739.

[23] Alsellami BM, Deshmukh PD. The recent trends in biometric traits authentication based on internet of things (IoT). In: Proceedings - international conference on artificial intelligence and smart systems. (March):2021, p. 1359–65. http://dx.doi.org/10.1109/ICAIS50930.2021.9396007.

[24] Mukhopadhyay SC, Tyagi SKS, Suryadevara NK, Piuri V, Scotti F, Zeadally S. Artificial intelligence-based sensors for next generation IoT applications: A review. IEEE Sens J 2021;21(22):24920–32. http://dx.doi.org/10.1109/JSEN.2021.3055618.

[25] Zhang D, Campbell JP, Maltoni D, Bolle RM. Guest editorial: Special issue on biometric systems. IEEE Trans Syst, Man Cybern C: Appl Rev 2005;35(3):273–5. http://dx.doi.org/10.1109/TSMCC.2005.848152.

[26] Ross A, Banerjee S, Chowdhury A. Security in smart cities: A brief review of digital forensic schemes for biometric data. Pattern Recognit Lett 2020;138:346–54. http://dx.doi.org/10.1016/j.patrec.2020.07.009.

[27] Karthick R, Ramkumar R, Akram M, Kumar MV. Overcome the challenges in bio-medical instruments using IOT - A review. Mater Today Proc 2021;45(January):1614–9. http://dx.doi.org/10.1016/j.matpr.2020.08.420.

[28] Moradi M, Moradkhani M, Tavakoli MB. Security-level improvement of IoT-based systems using biometric features. Wirel Commun Mob Comput 2022;2022(Idc). http://dx.doi.org/10.1155/2022/8051905.

[29] Chawla MN. AI, IOT and wearable technology for smart healthcare-A review. Int J Recent Res Aspects 2020;7(1):9–13.

[30] Mariani MM, Perez-Vega R, Wirtz J. AI in marketing, consumer research and psychology: A systematic literature review and research agenda. Psychol Mark 2022;39(4):755–76. http://dx.doi.org/10.1002/mar.21619.

[31] Fernández-Caramés TM, Fraga-Lamas P. Towards the internet-of-smart-clothing: A review on IoT wearables and garments for creating intelligent connected E-textiles. Electronics (Switzerland) 2018;7(12). http://dx.doi.org/10.3390/electronics7120405.

[32] Zhang Z, Ning H, Farha F, Ding J, Choo K-KR. Artificial intelligence in physiological characteristics recognition for internet of things authentication. Digit Commun Netw 2022. http://dx.doi.org/10.1016/j.dcan.2022.10.006.

[33] Liang Y, Samtani S, Guo B, Yu Z. Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. IEEE Internet Things J 2020;7(9):9128–43. http://dx.doi.org/10.1109/JIOT.2020.3004077.

[34] Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun Policy 2017;41(10):1027–38. http://dx.doi.org/10.1016/j.telpol.2017.09.003.

[35] Zhao K, Ge L. A survey on the internet of things security. In: Proceedings - 9th international conference on computational intelligence and security. IEEE; 2013, p. 663–7. http://dx.doi.org/10.1109/CIS.2013.145.

[36] Soutar C, Roberge D, Gilroy R, Stoianov A, Vijaya Kumar B. Biometric encryption. Biometr Technol Today 2007;15(3):11. http://dx.doi.org/10.1016/S0969-4765(07)70084-X.

[37] Jain AK, Nandakumar K. Biometric authentication: System security and user privacy. Computer 2012;45(11):87–92. http://dx.doi.org/10.1109/MC.2012.364.

[38] Adjabi I, Ouahabi A, Benzaoui A, Taleb-Ahmed A. Past, present, and future of face recognition: A review. Electronics (Switzerland) 2020;9(8):1–53. http://dx.doi.org/10.3390/electronics9081188.

[39] Israa A. Physiological biometric authentication systems, advantages, disadvantages and future development: A review. Int J Sci Technol Res 2015;1(1):7.

[40] Rub M, Herbst J, Lipps C, Schotten HD. No one acts like you: AI based behavioral biometric identification. In: Proceedings - 3rd international conference on next generation computing applications. (October). 2022, http://dx.doi.org/10.1109/NextComp55567.2022.9932247.

[41] Bock L. Identity Management with Biometrics: Explore the latest innovative solutions to provide secure identification and authentication. Packt Publishing Ltd; 2020.

[42] li Liu Y, Huang L, Yan W, Wang X, Zhang R. Privacy in AI and the IoT: The privacy concerns of smart speaker users and the Personal Information Protection Law in China. Telecommun Policy 2022;46(7):102334. http://dx.doi.org/10.1016/j.telpol.2022.102334.

[43] Chen Z, Feng X, Zhang S. Emotion detection and face recognition of drivers in autonomous vehicles in IoT platform. Image Vis Comput 2022;128:104569. http://dx.doi.org/10.1016/j.imavis.2022.104569.

[44] Chen Y, Zhao S, Zhou Y. Research on intelligent agricultural planting system based on internet of things technology. J Comput Commun 2018;06(06):54–60. http://dx.doi.org/10.4236/jcc.2018.66005.

[45] Matyáš V, Říha Z. Security of biometric authentication systems. In: 2010 International conference on computer information systems and industrial management applications. 2010, p. 19–28. http://dx.doi.org/10.1109/CISIM.2010.5643698.

[46] Awad AI, Baba K. Fingerprint singularity detection: A comparative study. In: Software engineering and computer systems: second international conference, ICSECS 2011, Kuantan, Pahang, Malaysia, June 27-29, 2011, proceedings, Part I. Vol. 2. Springer; 2011, p. 122–32. http://dx.doi.org/10.1007/978-3-642-22170-5_11.

[47] Atzori L, Iera A, Morabito G. The internet of things: A survey. Comput Netw 2010;54(15):2787–805. http://dx.doi.org/10.1016/j.comnet.2010.05.010.

[48] Vermesan O, Friess P. Internet of things: Converging technologies for smart environments and integrated ecosystems (river publishers series in communications). Internet of things. (January):2013, p. 45.

[49] Ali B, Awad AI. Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors 2018;18(3):1–17. http://dx.doi.org/10.3390/s18030817.

[50] Awad AI, Furnell S, Paprzycki M, Sharma S. Security in cyber-physical systems: Foundations and applications. In: Studies in systems, decision and control, Springer International Publishing; 2021.

[51] Roman R, Lopez J, Mambo M. Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. Future Gener Comput Syst 2018;78:680–98. http://dx.doi.org/10.1016/j.future.2016.11.009, arXiv:1602.00484.

[52] Kaur B, Dadkhah S, Shoeleh F, Neto ECP, Xiong P, Iqbal S, et al. Internet of Things (IoT) security dataset evolution: Challenges and future directions. Internet Things (Netherlands) 2023;22(March):100780. http://dx.doi.org/10.1016/j.iot.2023.100780.

[53] Ang KLM, Seng KP. Biometrics-based Internet of Things and Big Data design framework. Math Biosci Eng 2021;18(4):4461–76. http://dx.doi.org/10.3934/mbe.2021226.

[54] King J, Awad AI. A distributed security mechanism for resource-constrained IoT devices. Informatica (Slovenia) 2016;40(1):133–43.

[55] Alzahrani S, Alderaan J, Alatawi D, Alotaibi B. Continuous mobile user authentication using a hybrid CNN-Bi-LSTM approach. Comput Mater Contin 2023;75(1):651–67. http://dx.doi.org/10.32604/cmc.2023.035173.

[56] Dhillon PK, Kalra S. A lightweight biometrics based remote user authentication scheme for IoT services. J Inf Secur Appl 2017;34:255–70. http://dx.doi.org/10.1016/j.jisa.2017.01.003.

[57] Liao B, Ali Y, Nazir S, He L, Khan HU. Security analysis of IoT devices by using mobile computing: A systematic literature review. IEEE Access 2020;8:120331–50. http://dx.doi.org/10.1109/ACCESS.2020.3006358.

[58] Huang CE, Li YH, Aslam MS, Chang CC. Super-resolution generative adversarial network based on the dual dimension attention mechanism for biometric image super-resolution. Sensors 2021;21(23). http://dx.doi.org/10.3390/s21237817.

[59] Dhillon PK, Kalra S. Secure multi-factor remote user authentication scheme for Internet of Things environments. Int J Commun Syst 2017;30(16):1–20. http://dx.doi.org/10.1002/dac.3323.

[60] Subha R. Biometrics in internet of things (IoT) security. Int J Eng Res Gener Sci 2017;5(5):37–42.

[61] Bagga P, Mitra A, Das AK, Vijayakumar P, Park YH, Karuppiah M. Secure biometric-based access control scheme for future IoT-enabled cloud-assisted video surveillance system. Comput Commun 2022;195(June):27–39. http://dx.doi.org/10.1016/j.comcom.2022.08.003.

[62] Sarkar A, Singh BK. A review on performance,security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools Appl 2020;79(37–38):27721–76. http://dx.doi.org/10.1007/s11042-020-09197-7.

[63] Vermesan O, Friess P, Guillemin P, Gusmeroli S, Sundmaeker H, Bassi A, et al. Internet of things strategic research roadmap. Cyber Resilience Syst Netw 2009;2019(July 2016):1–150.

[64] Okoh E, Awad AI. Biometrics applications in e-Health security: A preliminary survey. In: Yin X, Ho K, Zeng D, Aickelin U, Zhou R, Wang H, editors. Health information science. Cham: Springer International Publishing; 2015, p. 92–103.

[65] Fatima K, Nawaz S, Mehrban S. Biometric authentication in health care sector: A survey. In: 2019 international conference on innovative computing. 2019, p. 1–10. http://dx.doi.org/10.1109/ICIC48496.2019.8966699.

[66] MacQuarrie AJ, Robertson C, Micalos P, Crane J, High R, Drinkwater E, et al. Fit for duty: the health status of New South Wales paramedics. Irish J Paramed 2018;3(2).

[67] Causa L, Tapia JE, Valenzuela A, Benalcazar D, Droguett EL, Busch C. Analysis of behavioural curves to classify iris images under the influence of alcohol, drugs, and sleepiness conditions. Expert Syst Appl 2024;242:122808. http://dx.doi.org/10.1016/j.eswa.2023.122808.

[68] Bera B, Das AK, Balzano W, Medaglia CM. On the design of biometric-based user authentication protocol in smart city environment. Pattern Recognit Lett 2020;138:439–46. http://dx.doi.org/10.1016/j.patrec.2020.08.017.

[69] Kairinos N. The integration of biometrics and AI. Biometr Technol Today 2019;2019(5):8–10. http://dx.doi.org/10.1016/S0969-4765(19)30069-4.

[70] Abdullahi SM, Sun S, Wang B, Wei N, Wang H. Biometric template attacks and recent protection mechanisms: A survey. Inf Fusion 2024;103:102144. http://dx.doi.org/10.1016/j.inffus.2023.102144.

[71] Deng P, Ge C, Wei H, Sun Y, Qiao X. Multimodal contrastive learning for face anti-spoofing. Eng Appl Artif Intell 2024;129:107600. http://dx.doi.org/10.1016/j.engappai.2023.107600.

[72] Shaheed K, Szczuko P, Kumar M, Qureshi I, Abbas Q, Ullah I. Deep learning techniques for biometric security: A systematic review of presentation attack detection systems. Eng Appl Artif Intell 2024;129:107569. http://dx.doi.org/10.1016/j.engappai.2023.107569.

[73] Smith M, Miller S. The ethical application of biometric facial recognition technology. AI Soc 2022;37(1):167–75. http://dx.doi.org/10.1007/s00146-021-01199-9.

[74] Killoran J, Cui YG, Park A, van Esch P, Kietzmann J. Can behavioral biometrics make everyone happy? Bus Horizons 2023;66(5):585–91. http://dx.doi.org/10.1016/j.bushor.2023.02.001.

[75] Jain T, Tomar U, Arora U, Jain S. IoT based biometric attendance system. Int J Electr Eng Technol 2020;11(2):156–61.

[76] Ahamed F, Farid F, Suleiman B, Jan Z, Wahsheh LA, Shahrestani S. An intelligent multimodal biometric authentication model for personalised health-care services. Future Internet 2022;14(8):1–28. http://dx.doi.org/10.3390/fi14080222.

[77] Guo Z, Karimian N, Tehranipoor MM, Forte D. Hardware security meets biometrics for the age of IoT. In: Proceedings - IEEE international symposium on circuits and systems. 2016-July, (i):2016, p. 1318–21. http://dx.doi.org/10.1109/ISCAS.2016.7527491.

[78] Hamidi H. An approach to develop the smart health using Internet of Things and authentication based on biometric technology. Future Gener Comput Syst 2019;91:434–49. http://dx.doi.org/10.1016/j.future.2018.09.024.

[79] Farid F, Elkhodr M, Sabrina F, Ahamed F, Gide E. A smart biometric identity management framework for personalised iot and cloud computing-based healthcare services. Sensors (Switzerland) 2021;21(2):1–18. http://dx.doi.org/10.3390/s21020552.

[80] Obaidat MS, Traore I, Woungang I. Biometric security and Internet of Things (IoT). In: Biometric-based physical and cybersecurity systems. (October):2018, p. 1–590. http://dx.doi.org/10.1007/978-3-319-98734-7.

[81] Chen S, Wen H, Wu J, Xu A, Jiang Y, Song H, et al. Radio frequency fingerprint-based intelligent mobile edge computing for internet of things authentication. Sensors (Switzerland) 2019;19(16). http://dx.doi.org/10.3390/s19163610.

[82] Das AK, Wazid M, Kumar N, Vasilakos AV, Rodrigues JJ. Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment. IEEE Internet Things J 2018;5(6):4900–13. http://dx.doi.org/10.1109/JIOT.2018.2877690.

[83] Anand A, Rani S, Anand D, Aljahdali HM, Kerr D. An efficient CNN-based deep learning model to detect malware attacks (CNN-DMA) in 5G-IoT healthcare applications. Sensors 2021;21(19). http://dx.doi.org/10.3390/s21196346.

[84] P. Chandel P, Kumar R. Internet of things for the prevention of black hole using fingerprint authentication and genetic algorithm optimization. Int J Comput Netw Inf Secur 2018;10(8):17–26. http://dx.doi.org/10.5815/ijcnis.2018.08.02.

[85] Abosata N, Al-Rubaye S, Inalhan G, Emmanouilidis C. Internet of things for system integrity: A comprehensive survey on security, attacks and counter-measures for industrial applications. Sensors 2021;21(11). http://dx.doi.org/10.3390/s21113654.

[86] Yaacoub J-pA, Noura HN, Salman O, Chehab A. Ethical hacking for IoT : Security issues , challenges , na ur l P re of. In: Internet of things and cyber–physical systems. KeAi Communications Co. Ltd; 2023, http://dx.doi.org/10.1016/j.iotcps.2023.04.002.

[87] Meena G, Choudhary S. Biometric authentication in internet of things : A conceptual view. J Stat Manag Syst 2019;22(4):643–52. http://dx.doi.org/10.1080/09720510.2019.1609722.

[88] Li B, Feng Y, Xiong Z, Yang W, Liu G. Research on AI security enhanced encryption algorithm of autonomous IoT systems. Inform Sci 2021;575:379–98. http://dx.doi.org/10.1016/j.ins.2021.06.016.

[89] Splinter R. EBiometrics: Data acquisition and physiological sensing. In: HONET 2021 - IEEE 18th international conference on smart communities: improving quality of life using ICT, IoT and AI. (Honet):IEEE; 2021, p. 112–5. http://dx.doi.org/10.1109/HONET53078.2021.9615465.

[90] Al-Assam H, Hassan W, Zeadally S. Automated biometric authentication with cloud computing. In: Biometric-based physical and cybersecurity systems. 2018, p. 455–75. http://dx.doi.org/10.1007/978-3-319-98734-7_18.

[91] Elordi U, Lunerti C, Unzueta L, Goenetxea J, Aranjuelo N, Bertelsen A, et al. Designing automated deployment strategies of face recognition solutions in heterogeneous IoT platforms. Information (Switzerland) 2021;12(12). http://dx.doi.org/10.3390/info12120532.

[92] Lancelot Miltgen C, Popovič A, Oliveira T. Determinants of end-user acceptance of biometrics: Integrating the "big 3" of technology acceptance with privacy context. Decis Support Syst 2013;56(1):103–14. http://dx.doi.org/10.1016/j.dss.2013.05.010.

[93] Oblak T, Haraksim R, Beslay L, Peer P. Probabilistic fingermark quality assessment with quality region localisation. Sensors 2023;23(8):1–22. http://dx.doi.org/10.3390/s23084006.

[94] Ortega-Rodríguez J, Gómez-González JF, Pereda E. Selection of the minimum number of EEG sensors to guarantee biometric identification of individuals. Sensors 2023;23(9):1–19. http://dx.doi.org/10.3390/s23094239.

[95] de Melo F, Neto HC, da Silva HP. System on chip (SoC) for invisible electrocardiography (ECG) biometrics. Sensors 2022;22(1):1–16. http://dx.doi.org/10.3390/s22010348.

[96] Mitro N, Argyri K, Pavlopoulos L, Kosyvas D, Karagiannidis L, Kostovasili M, et al. AI-enabled smart wristband providing real-time vital signs and stress monitoring. Sensors 2023;23(5):1–26. http://dx.doi.org/10.3390/s23052821.

[97] Saoji SU, Kumar N, Jayakumar, Gupta V, Agarwal P, Astogi P. Attendance management system using deep learning and facial recognition technique. Int J Innov Technol Explor Eng 2019;8(10):4097–101. http://dx.doi.org/10.35940/ijitee.J9423.0881019.

[98] Sulavko A. Biometric-based key generation and user authentication using acoustic characteristics of the outer ear and a network of correlation neurons. Sensors 2022;22(23). http://dx.doi.org/10.3390/s22239551.

[99] Albaladejo-González M, Ruipérez-Valiente JA, Gómez Mármol F. Evaluating different configurations of machine learning models and their transfer learning capabilities for stress detection using heart rate. J Ambient Intell Humaniz Comput 2023;14(8):11011–21. http://dx.doi.org/10.1007/s12652-022-04365-z.

[100] Aquino G, Costa MG, Costa Filho CF. Explaining one-dimensional convolutional models in human activity recognition and biometric identification tasks. Sensors 2022;22(15). http://dx.doi.org/10.3390/s22155644.

[101] Moon Y, Ryoo I, Kim S. Face antispoofing method using color texture segmentation on FPGA. Secur Commun Netw 2021;2021. http://dx.doi.org/10.1155/2021/9939232.

[102] Peña A, Serna I, Morales A, Fierrez J, Ortega A, Herrarte A, et al. Human-centric multimodal machine learning: Recent advances and testbed on AI-based recruitment. SN Comput Sci 2023;4(5). http://dx.doi.org/10.1007/s42979-023-01733-0, arXiv:2302.10908.

[103] Fiolka J, Bernacki K, Farah A, Popowicz A. Multi-wavelength biometric acquisition system utilizing finger vasculature NIR imaging. Sensors 2023;23(4):1–14. http://dx.doi.org/10.3390/s23041981.

[104] Rodriguez P, Cucurull G, Gonzalez J, Gonfaus JM, Nasrollahi K, Moeslund TB, et al. Deep pain: Exploiting long short-term memory networks for facial expression classification. IEEE Trans Cybern 2022;52(5):3314–24. http://dx.doi.org/10.1109/TCYB.2017.2662199.

[105] Kang T, Oh KI, Lee JJ, Park BS, Oh W, Kim SE. Measurement and analysis of human body channel response for biometric recognition. IEEE Trans Instrum Meas 2021;70:1–12. http://dx.doi.org/10.1109/TIM.2021.3106132.

[106] Sedik A, Tawalbeh L, Hammad M, El-Latif AA, El-Banby GM, Khalaf AA, et al. Deep learning modalities for biometric alteration detection in 5g networks-based secure smart cities. IEEE Access 2021;9:94780–8. http://dx.doi.org/10.1109/ACCESS.2021.3088341.

[107] Wang D, Yu H, Wang D, Li G. Face recognition system based on CNN. In: Proceedings - 2020 international conference on computer information and big data applications. 2020, p. 470–3. http://dx.doi.org/10.1109/CIBDA50819.2020.00111.

[108] Girmay S, Samsom F, Khattak AM. AI based login system using facial recognition. In: 2021 5th Cyber security in networking conference. IEEE; 2021, p. 107–9. http://dx.doi.org/10.1109/CSNet52717.2021.9614281.

[109] Krishna MYS, Arya A, Ansari S, Awasya S, Sushakar J, Uikey N. Real time door unlocking system using facial biometrics based on IoT and python. In: 2023 IEEE international students' conference on electrical, electronics and computer science. IEEE; 2023, p. 1–5. http://dx.doi.org/10.1109/SCEECS57921.2023.10063142.

[110] Meddeb H, Abdellaoui Z, Houaidi F. Development of surveillance robot based on face recognition using Raspberry-PI and IOT. Microprocess Microsyst 2023;96(November 2022):104728. http://dx.doi.org/10.1016/j.micpro.2022.104728.

[111] Wells A, Usman AB. Trust and voice biometrics authentication for internet of things. Int J Inf Secur Priv 2023;17(1):1–28. http://dx.doi.org/10.4018/IJISP.322102.

[112] Jaswal G, Bharadwaj R, Tiwari K, Thapar D, Goyal P, Nigam A. AI-biometric-driven smartphone app for strict post-COVID home quarantine management. IEEE Consum Electron Mag 2021;10(3):49–55. http://dx.doi.org/10.1109/MCE.2020.3039035.

[113] Sidiropoulos GK, Papakostas GA. Machine biometrics-towards identifying machines in a smart city environment. In: 2021 IEEE world AI IoT congress. (1):IEEE; 2021, p. 197–201. http://dx.doi.org/10.1109/AIIoT52608.2021.9454230.

[114] Annadurai C, Nelson I, Devi KN, Manikandan R, Jhanjhi NZ, Masud M, et al. Biometric authentication-based intrusion detection using artificial intelligence internet of things in smart city. Energies 2022;15(19). http://dx.doi.org/10.3390/en15197430.

[115] Jain A, Ross A, Prabhakar S. An introduction to biometric recognition. IEEE Trans Circuits Syst Video Technol 2004;14(1):4–20. http://dx.doi.org/10.1109/TCSVT.2003.818349.

[116] Jain A, Ross A, Nandakumar K. Introduction to biometrics. Springer US; 2011.

[117] Hintze D, Füller M, Scholz S, Findling RD, Muaaz M, Kapfer P, et al. CORMORANT: Ubiquitous risk-aware multi-modal biometric authentication across mobile devices. Proc ACM Interact Mob Wearable Ubiquitous Technol 2019;3(3). http://dx.doi.org/10.1145/3351243.

[118] Mosenia A, Jha NK. A comprehensive study of security of internet-of-things. IEEE Trans Emerg Top Comput 2017;5(4):586–602. http://dx.doi.org/10.1109/TETC.2016.2606384.

[119] Nguyen V-L, Lin P-C, Hwang R-H. Energy depletion attacks in low power wireless networks. IEEE Access 2019;7:51915–32. http://dx.doi.org/10.1109/ACCESS.2019.2911424.

[120] Abdelrahman Y, Khamis M, Schneegass S, Alt F. Stay cool! understanding thermal attacks on mobile-based user authentication. In: Proceedings of the 2017 CHI conference on human factors in computing systems. New York, NY, USA: Association for Computing Machinery; 2017, p. 3751—-3763. http://dx.doi.org/10.1145/3025453.3025461.

[121] Tomić I, McCann JA. A survey of potential security issues in existing wireless sensor network protocols. IEEE Internet Things J 2017;4(6):1910–23. http://dx.doi.org/10.1109/JIOT.2017.2749883.

[122] Phillips PJ, Przybocki M. Four principles of explainable AI as applied to biometrics and facial forensic algorithms. 2020, arXiv:2002.01014.

[123] Ribeiro MT, Singh S, Guestrin C. "Why should i trust you?" Explaining the predictions of any classifier. In: Proceedings of the ACM SIGKDD international conference on knowledge discovery and data mining. 13-17-August-2016. 2016, p. 1135–44. http://dx.doi.org/10.1145/2939672.2939778.

[124] Abadade Y, Temouden A, Bamoumen H, Benamar N, Chtouki Y, Hafid AS. A comprehensive survey on TinyML. IEEE Access 2023;1–31. http://dx.doi.org/10.1109/ACCESS.2023.3294111.

[125] Tang L, Li H, Yan C, Zheng X, Ji R. Survey on neural architecture search. J Image Graph 2021;26(2):245–64. http://dx.doi.org/10.11834/jig.200202.

[126] Shi Q, Dong B, He T, Sun Z, Zhu J, Zhang Z, et al. Progress in wearable electronics/photonics—Moving toward the era of artificial intelligence and internet of things. InfoMat 2020;2(6):1131–62. http://dx.doi.org/10.1002/inf2.12122.

[127] Nam KH, Kim DH, Choi BK, Han IH. Internet of things, digital biomarker, and artificial intelligence in spine: Current and future perspectives. Neurospine 2019;16(4):705–11. http://dx.doi.org/10.14245/ns.1938388.194.

[128] Mondal TG, Chen G. Artificial intelligence in civil infrastructure health monitoring—Historical perspectives, current trends, and future visions. Front Built Environ 2022;8(September):1–24. http://dx.doi.org/10.3389/fbuil.2022.1007886.

[129] Esenogho E, Djouani K, Kurien AM. Integrating artificial intelligence internet of things and 5G for next-generation smartgrid: A survey of trends challenges and prospect. IEEE Access 2022;10:4794–831. http://dx.doi.org/10.1109/ACCESS.2022.3140595.