Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9, 172-194
2025
Publisher: Learning Gate
DOI: 10.55214/2576-8484.v9i9.9781

A systematic literature review on integrating contactless biometrics into online learning environments

Samukeliswe Londeka Xaba[1], Halleluyah Oluwatobi Aworinde[2*], Brett van Niekerk[3]
[1,2,3]Information Technology Department, Durban University of Technology, Durban KwaZulu-Natal, South Africa;
21801977@dut4life.ac.za (S.L.X.) halleluyaha@dut.ac.za (H.O.A.) brettV@dut.ac.za (B.V.N.).

Abstract: The rapid expansion of online learning platforms has created significant challenges in ensuring secure and seamless user authentication. Traditional methods, such as passwords and PINs, are vulnerable to security breaches and inefficiencies, prompting the exploration of contactless biometric technologies as viable alternatives. This systematic literature review examines the integration of contactless biometrics—such as facial recognition, voice patterns, and behavioral traits—into online learning environments, emphasizing their effectiveness, advantages, and challenges. This review analyzed 44 peer-reviewed studies from 2010 to 2024. Findings from the review show that contactless biometrics enhance security and user experience but face adoption barriers, such as privacy concerns, algorithmic biases, and technical limitations. Multimodal systems (e.g., combining facial recognition and keystroke dynamics) demonstrate promise in balancing accuracy and scalability, especially in high-stakes assessments. Ethical and regulatory frameworks, including GDPR compliance and bias mitigation, are crucial for responsible deployment. The study identifies gaps in research on Massive Open Online Courses (MOOCs) and underscores the urgent need for scalable, inclusive solutions. Recommendations include hybrid authentication models, inclusive design for diverse learners, and iterative testing to enhance fairness and usability. By synthesizing current advancements and challenges, this review provides actionable insights into the responsible integration of contactless biometrics in online learning for educators, developers, and policymakers. It contributes to the discourse on ethical deployment, regulatory compliance, and inclusive technological design, offering a foundation for future research and innovation in digital authentication.

Keywords: *Authentication, Contactless biometrics, Information security, MOOCs, Multimodal systems, Online learning, Privacy.*

1. Introduction

The rise of online learning platforms has profoundly transformed the delivery of education, enhancing its flexibility and accessibility for students worldwide. Technological advancements have driven institutions to offer remote courses, allowing students to learn at their own pace from any location [1]. However, the growth of digital education has introduced new challenges, particularly concerning the safety of online learning platforms. User identity verification remains a critical concern, making it essential to ensure that only authorized users can access course materials and assessments.

Due to the rapid advancement of online learning environments [1, 2] education's flexibility and accessibility have significantly improved. However, this expansion has raised growing concerns about user identity verification and security. It is crucial to ensure that only authorized users can access learning platforms and participate in evaluations, especially as education rapidly shifts to digital and remote formats. The search for more reliable and seamless alternatives to traditional authentication methods, such as passwords and PINs, has become essential due to their limitations in both security and user experience.

History: Received: 25 June 2025; Revised: 8 August 2025; Accepted: 12 August 2025; Published: 2 September 2025
* Correspondence: halleluyaha@dut.ac.za

Conventional methods of identity verification, such as passwords and PINs, have been widely used for online security. However, they come with significant drawbacks. They are susceptible to hacks, password fatigue, and human error, leading to increased security threats and a subpar user experience [3, 4]. With the rise of online learning, there is an increasing need for improved security measures, prompting educational institutions and technology developers to create more secure alternatives. Biometric technology has emerged as a viable solution to these problems, offering a more secure and convenient method of authentication. Biometrics rely on distinct physiological or behavioral traits, such as fingerprints, facial recognition, and voice patterns, to verify user identities. [4, 5] These technologies are more secure than traditional methods because they are difficult to forge or steal. Additionally, biometric authentication enhances the user experience by eliminating the need for

passwords and reducing the likelihood of forgetting credentials. Biometrics utilize unique physiological or behavioral characteristics such as fingerprints, facial recognition, and speech patterns, providing more secure and intuitive authentication solutions [4]. Contactless biometrics have gained attention for remote access scenarios due to their practicality and non-intrusive nature. These technologies are ideal for online learning systems where user-friendliness and hygiene are essential, as they enable user authentication without any direct physical interaction.

Contactless biometrics have gained significant attention in biometric technologies due to their efficiency in remote learning environments. Unlike traditional biometrics that require physical contact, contactless methods such as facial and voice recognition enable user authentication without intrusion. [5, 6]. This is particularly beneficial in academic settings, where cleanliness and user-friendly features are crucial, especially in light of the COVID-19 pandemic.

Contactless biometrics can enhance security and user experience when integrated into online learning environments [5-7]. However, deploying this technology is not without challenges; issues such as privacy, technological limitations, and ethical considerations arise. Therefore, to understand the current state of research, identify best practices, and recognize gaps that require attention, it is essential to conduct a comprehensive assessment of the existing literature.

While there are potential advantages, integrating contactless biometrics into online learning environments poses several challenges. Privacy concerns are significant since biometric information is highly sensitive, and its management must adhere to data protection laws. Moreover, ethical issues may arise from potential misuse or bias in biometric systems, alongside technological limitations that could impact their accuracy and reliability. Implementing biometric systems also requires substantial technical infrastructure and financial investment, which may not be feasible for all educational institutions.

The growing popularity of virtual learning environments has highlighted significant security and user experience issues. Passwords and PINs exemplify traditional authentication systems that are vulnerable to security risks and user management challenges. Contactless biometric technologies, such as facial recognition and fingerprint scanning, have emerged as viable options as educational institutions seek more secure and user-friendly solutions. However, there is still a lack of research on how these technologies can be integrated into online learning environments, raising concerns about their effectiveness, scalability, and impact on user experience. Consequently, this study addresses the following primary research questions:

RQ1 What are the key findings from recent studies on the use of contactless biometric technology in online learning environments?

RQ2 What are the primary benefits and challenges of using contactless biometrics to enhance security on online education platforms?

RQ3 What frameworks and best practices are available for integrating contactless biometric technology into online educational platforms?

RQ4 How can contactless biometrics be effectively utilized to improve user experience and security for educational institutions and technology developers?

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 172-194, 2025
DOI: 10.55214/2576-8484.v9i9.9781

This study reviews and evaluates existing research to offer insights into the benefits, challenges, and future directions of implementing contactless biometrics in educational settings. The findings contribute to the ongoing discussion about enhancing security and usability in online learning environments through innovative biometric solutions. It presents a systematic literature review on the integration of contactless biometrics into these environments. The study aims to explore how these technologies can bolster security measures while optimizing the user experience.

This study examines cutting-edge research from 2010 to 2024 on the integration of contactless biometric technologies in e-learning environments, evaluating the effects on user privacy, data security, and overall usability. Therefore, the main contributions of this study are as follows:

1. It offers a thorough review of current research, highlighting the benefits and drawbacks of these technologies while providing guidance on their effective use.
2. It examines the integration of contactless biometric solutions to improve accessibility for various user groups, including those with disabilities, while reducing disruptions to the learning process.
3. It provides effective strategies for integrating biometric technologies into online educational platforms, offering valuable recommendations for teachers, programmers, and decision-makers.
4. It provides a thorough assessment of the trade-offs between improving security and safeguarding users' rights, along with recommendations for responsible implementation.
5. The study identifies gaps in the existing literature and suggests future research aimed at improving the accuracy of biometric systems in various learning environments, addressing bias issues, and exploring new biometric technologies.

While Massive Open Online Courses (MOOCs) now serve over 220 million learners globally [6], their unique authentication challenges remain understudied – a gap this review addresses.

The remainder of this article is structured as follows: Section 2 reviews the literature on integrating contactless biometric technologies into learning environments. Section 3 outlines the materials and procedures used in this study. In Section 3, the search strategy, appropriateness measures, online resources, selected articles, data collection techniques, and evaluation methods are described in detail. Section 4 analyzes the findings, including the results of the search method, research characteristics, and limitations. Section 5 summarizes the remaining sections of this work.

2. Related Works

Biometrics refers to the automated identification of individuals through their unique biological and behavioral traits. These traits can be categorized as either physiological or behavioral [7, 8] Physiological biometrics include characteristics that are unique to an individual's body, such as fingerprints, facial features, iris patterns, and DNA. In contrast, behavioral biometrics examine patterns in a person's actions or behaviors, including voice patterns, typing speed, and gait [4, 5].

Non-contact biometrics, a form of biometric technology, involves collecting physiological or behavioral data without any physical contact with the system [7-9]. Unlike traditional fingerprint scanning, contactless biometrics do not require direct interaction with a sensor; instead, they utilize remote sensing techniques to gather information. Examples include facial recognition, voice recognition, and iris scanning. These technologies are particularly significant in today's context, where hygiene and user convenience are paramount, especially in sectors like education, where regular physical interactions with devices are impractical.

This section examines the current research status of integrating contactless biometrics in online learning environments, analyzing the benefits, challenges, and potential future directions of this technology.

2.1. Contactless Biometrics in Education

The adoption of contactless biometrics (e.g., facial recognition and voice patterns) has grown alongside digital learning platforms, particularly for identity verification in high-stakes assessments [8]. While most studies focus on traditional online courses, MOOCs (Massive Open Online Courses) present unique challenges due to their open-access models and diverse global learner demographics. For instance:

- Scalability: MOOCs require solutions that operate across various devices and bandwidth conditions [1], yet current biometric systems frequently assume a standard model.
- Proctoring: Platforms such as Coursera utilize AI proctoring with facial recognition but encounter criticism regarding privacy and bias [9].

2.2. Behavioral Biometrics

Behavioral traits like keystroke dynamics are gaining traction for non-intrusive authentication. Recent research by Hinbarji [10] demonstrates their potential for continuous verification in self-paced MOOCs, although accuracy declines in low-engagement scenarios.

2.3. Ethical and Accessibility Challenges

Privacy concerns dominate biometric literature [11], but MOOCs amplify these issues due to global data laws: GDPR compliance conflicts with regions lacking biometric regulations. Moreover, disability access, such as voice recognition, may exclude learners with speech impairments, creating a critical gap in MOOC inclusivity [12].

2.4. Comparative Efficacy of Contactless Biometric Modalities

Recent studies show significant performance variations among biometric types used in online learning environments (Table 1). These differences are especially important in MOOC settings due to their diverse user base and technical limitations.

Table 1.
Biometric Modality Comparison for Online Learning Environment.

Modality	Accuracy (F1 Score)	Hardware Requirements	MOOC Suitability	Key Limitations
Facial Recognition Azimi [13]	0.92	Webcam (720p+)	High (proctoring)	Lighting sensitivity, racial bias Buolamwini and Gebru [23]
Voice Recognition Patel [14]	0.81	Microphone	Medium (verbal exams)	Background noise, speech disorders
Iris Scanning Raghavendra, et al. [15]	0.95	IR camera	Low (cost-prohibitive)	Requires specialized hardware
Keystroke Dynamics Hinbarji [10]	0.76	Keyboard/touchscreen	High (scalability)	Low discriminative power

While iris scanning achieves the highest accuracy (0.95 F1), its hardware requirements make it impractical for scaling MOOCs. Facial recognition offers the best balance (0.92) but requires bias mitigation. Keystroke dynamics show promise for MOOC scalability but necessitate longer authentication periods [16]. Voice recognition accuracy declines to 0.68 in noisy environments [14], which poses challenges for learners in informal settings. Although [13] reports 92% facial recognition accuracy, [14] notes this drops to 68% in low-light MOOC environments.

This comparative analysis emphasizes the necessity of adaptive multimodal systems in MOOCs, where no single modality effectively addresses all use cases.

3. Method

This section covers the research design, eligibility requirements, information sources and searches, study selection, data collection techniques, and data retrieval and analysis.

3.1. Research Design

This research employs a systematic literature review (SLR) method to thoroughly and impartially evaluate the current literature on the integration of contactless biometric technologies in online educational settings. Following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, this review, as shown in Figure 1, aims to summarize existing research, identify areas for improvement, and highlight effective integration strategies.

PRISMA is highly regarded in academia for its systematic reviews because of its transparent framework that enables consistent and comprehensive reporting. In this review, employing PRISMA provides a clear understanding of study selection, filtering, and inclusion, allowing future researchers to replicate the review process or build upon its conclusions. The credibility of the findings is further enhanced by the PRISMA guidelines, which aim to minimize biases in selecting studies and extracting data.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 172-194, 2025
DOI: 10.55214/2576-8484.v9i9.9781

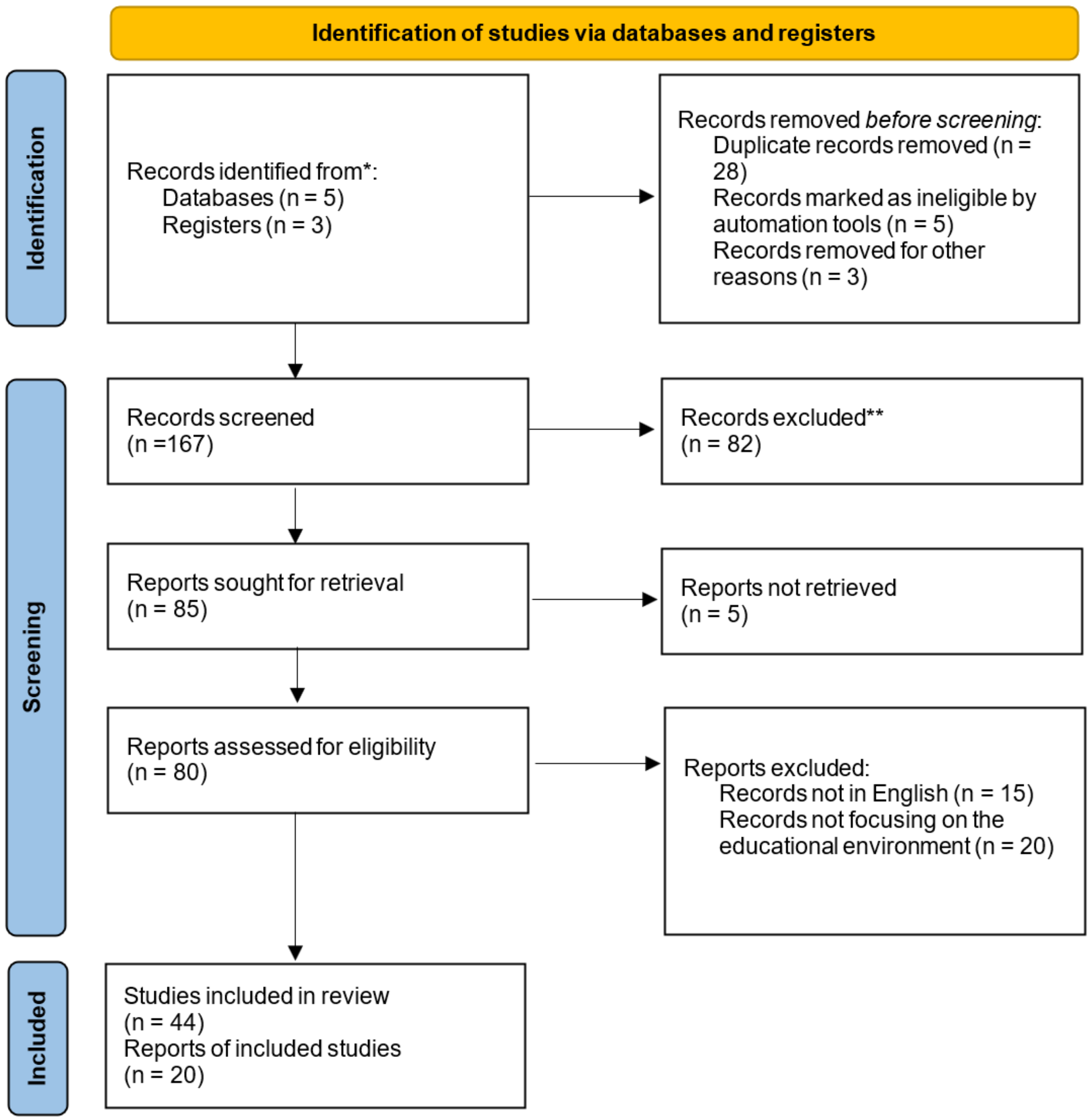

Figure 1.
PRISMA flow diagram of article selection used in the study.

The review examined research from 2010 to 2024, spanning 14 years, that illustrates the rise of online learning and technological advancements, particularly after 2010, when online education gained global popularity. Furthermore, the analysis focuses on peer-reviewed literature to maintain a high level of academic rigor. The review explores the theoretical and practical applications of contactless biometrics in online education through empirical studies, case studies, and technical evaluations.

3.2. Search Strategy and String

A comprehensive search strategy was employed to retrieve relevant studies. The consulted databases include:

- IEEE Xplore highlights technical literature and advancements in biometrics and security.
- Scopus offers a wide range of peer-reviewed articles across various fields, including education and technology.
- Web of Science is a database that focuses on high-impact studies related to e-learning security and authentication systems.
- Google Scholar provides extensive access to a wide range of academic articles and conference papers.
- PubMed explores possible intersections between biometric security and digital education.

A systematic search strategy employed the following string to capture relevant literature:

("contactless biometrics" OR "biometric technology" OR "biometric authentication") AND ("online learning" OR "virtual learning" OR "e-learning" OR "online education") AND ("security" OR "user experience" OR "framework")

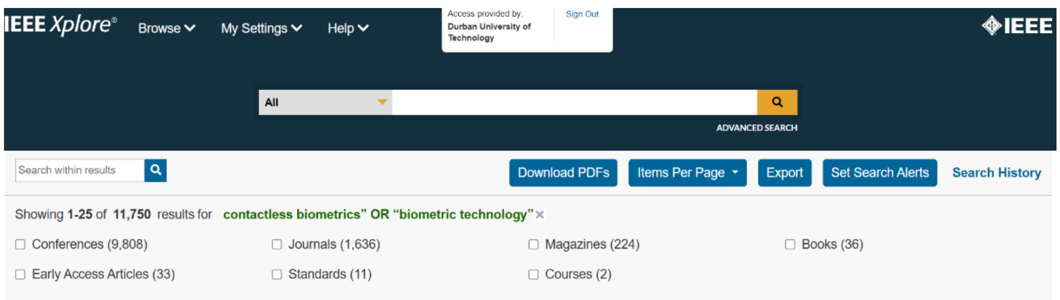

Figure 2.
Sample Search Preferences.

This sequence was developed by analyzing keywords associated with the primary areas of the research queries and topics. Boolean operators such as "AND" and "OR" were employed to encompass a wide and inclusive array of related research studies.

3.3. Eligibility Criteria

The work analyzed all studies that focus on the use of contactless biometric technologies in online learning environments. The admission criteria were published (i) between 2010 and 2024, (ii) in English, (iii) in a peer-reviewed professional publication, and (iv) in a preprint journal. Unpublished thesis and dissertation research, along with conference articles, non-English research, and studies not specifically centered on the application of contactless biometric technologies in online or virtual learning environments- except when translated metadata confirmed relevance (n = 3)- were excluded from the review. Tables 2 and 3 display the eligibility criteria used in the review regarding inclusion and exclusion processes.

Table 2.
Inclusion Criteria.

Code	Description
IC 1	Studies that focus on the use of contactless biometric technologies with online learning environments.
IC 2	Peer-reviewed articles, conference papers, published between 2010 and 2024.
IC 3	Articles available in English.
IC 4	Research involving students, teachers, or faculty in tertiary education, secondary education, or internet-based learning environment.
IC 5	Research that examines the practical application, difficulties in combining, or modifications of touchless biometric technology in educational systems.
IC 6	Research that presents real-life data on the usability, precision, student satisfaction, and security efficacy of biometrics in online environments.

Table 3.
Exclusion Criteria.

Code	Description
EC 1	Studies that do not specifically focus on the application of contactless biometric technologies within online or virtual learning environments
EC 2	Abstract-only articles or studies behind paywalls without access to full text.
EC 3	Studies that discuss biometrics in other sectors like healthcare, finance, or general security without educational context.
EC 4	Studies focusing solely on theoretical or conceptual frameworks without presenting any practical implementation or results.
EC 5	Research lacking empirical data or specific metrics on usability, accuracy, user satisfaction, or security performance of biometrics in online learning environment

3.4. Information Source and Search

IEEE Xplore, Scopus, Web of Science, Google Scholar, and PubMed were used to search for literature. Many results in the electronic databases, as previously mentioned, were completed in 2024 with the following search phrases: (“contactless biometrics” OR “biometric technology” OR “biometric authentication”) AND (“online learning” OR “virtual learning” OR “e-learning” OR “online education”) AND (“security” OR “user experience” OR “framework”). Figure 3 illustrates the distribution by publishing source type. Figures 3, 4, and 5 showcase the outcomes of these processes.

Figure 5 illustrates the various types of documents categorized as articles, journals, conference papers, books, reports, preprints, and theses. The graph shows that most of the analysis concentrated on journal publications.

3.5. Study Selection

The search aimed to curate an initial list of studies for extensive assessment. The articles were then reviewed to determine their relevance and whether they could address the established research questions, which spanned from 2010 to 2024 (see Figures 1 to 5). Tables 4 through 10 present some of the selected papers based on the study focus.

The research selection used a systematic screening and filtering process to ensure relevance and methodological integrity.

Step 1: Duplicate Removal

- Reference management systems, such as EndNote, were used to find and eliminate duplicate research from several databases.
- 28 duplicate records were removed.

Step 2: Title & Abstract Screening

- Titles and abstracts of 167 studies were screened based on relevance to biometric authentication in online learning.

ISSN: 2576-8484
Vol. 9, No. 9: 172-194, 2025
DOI: 10.55214/2576-8484.v9i9.9781

- 82 studies were excluded for not addressing biometric integration in online education.

Step 3: Full-Text Review for Eligibility

- 85 studies were selected for full-text assessment.
- 5 studies could not be retrieved, leaving 80 for further review.
- 35 studies were excluded based on:

15 were not in English.
20 did not focus on e-learning environments.
Step 4: Final Inclusion

- A total of 44 studies met all inclusion criteria and were included in the systematic review.
- Twenty of these studies provided detailed empirical data on the usability, accuracy, and security of biometrics in online learning.

3.6. Data Synthesis

To summarize the findings, a mixed-methods approach was utilized:

- Qualitative Synthesis – A thematic analysis was conducted to identify common advantages, challenges, and best practices in biometric authentication for online learning.
- Quantitative Synthesis – Statistical results such as authentication accuracy, user satisfaction rates were compiled to compare different biometric technologies.

3.7. Quality Assessment

To ensure that only high-quality evidence is included, a quality evaluation was conducted using a standardized checklist. Each study was assessed based on several criteria by employing relevant research questions:

1. What are the key findings from recent studies on integrating contactless biometric technology into online learning environments?
   This question aims to summarize findings, innovations, and advancements in the integration of biometric technologies into online education.
2. What are the primary benefits and challenges of using contactless biometrics to enhance security on online education platforms?
   This question seeks to examine the benefits of contactless biometrics for secure online learning platforms, along with any challenges or limitations they may pose.
3. What frameworks and best practices exist for integrating contactless biometric technology into online educational platforms?
   This question examines the established models, best practices, or industry standards that inform the integration of biometric technology in e-learning.
4. How can contactless biometrics be effectively used to enhance user experience and security for educational institutions and technology developers?
   This question explores potential applications of biometric technology to improve both security and usability for educational stakeholders.

The methodological quality of each study was evaluated using established critical appraisal tools.

4. Results and Discussion

This section presents data that have been collected and analyzed, provides an overview of the reviews, describes the search technique developed during the study, and outlines the drawbacks of the review study.

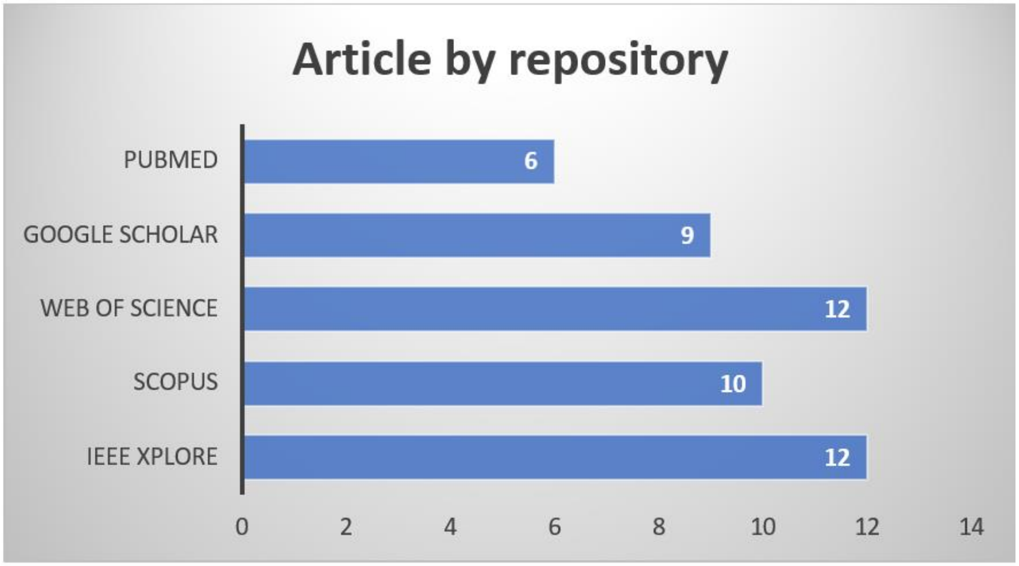

Figure 3.
Analysed Sources.

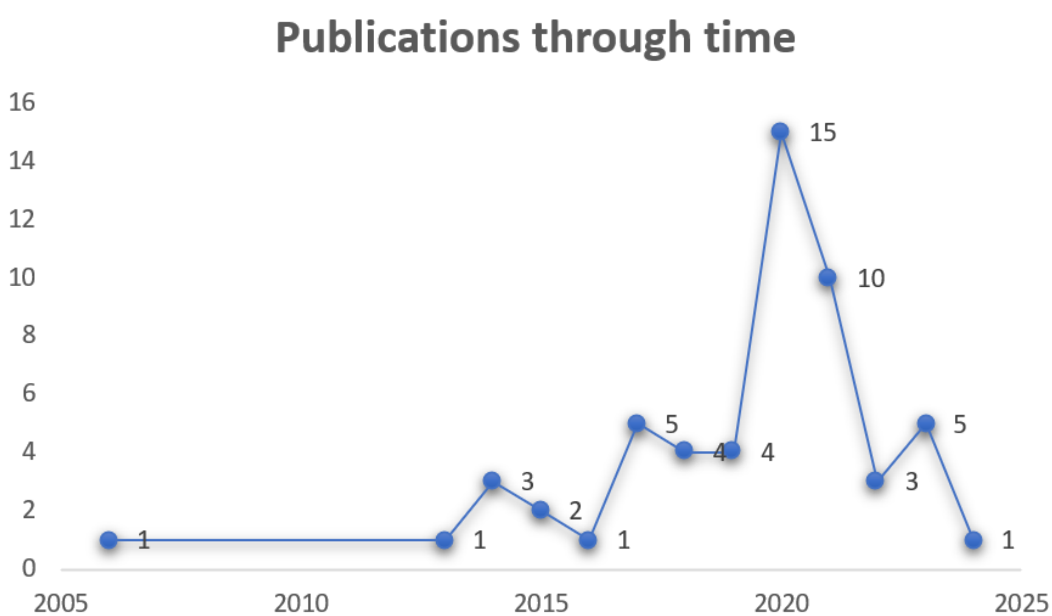

Figure 4.
Selected Number of Publications per year.

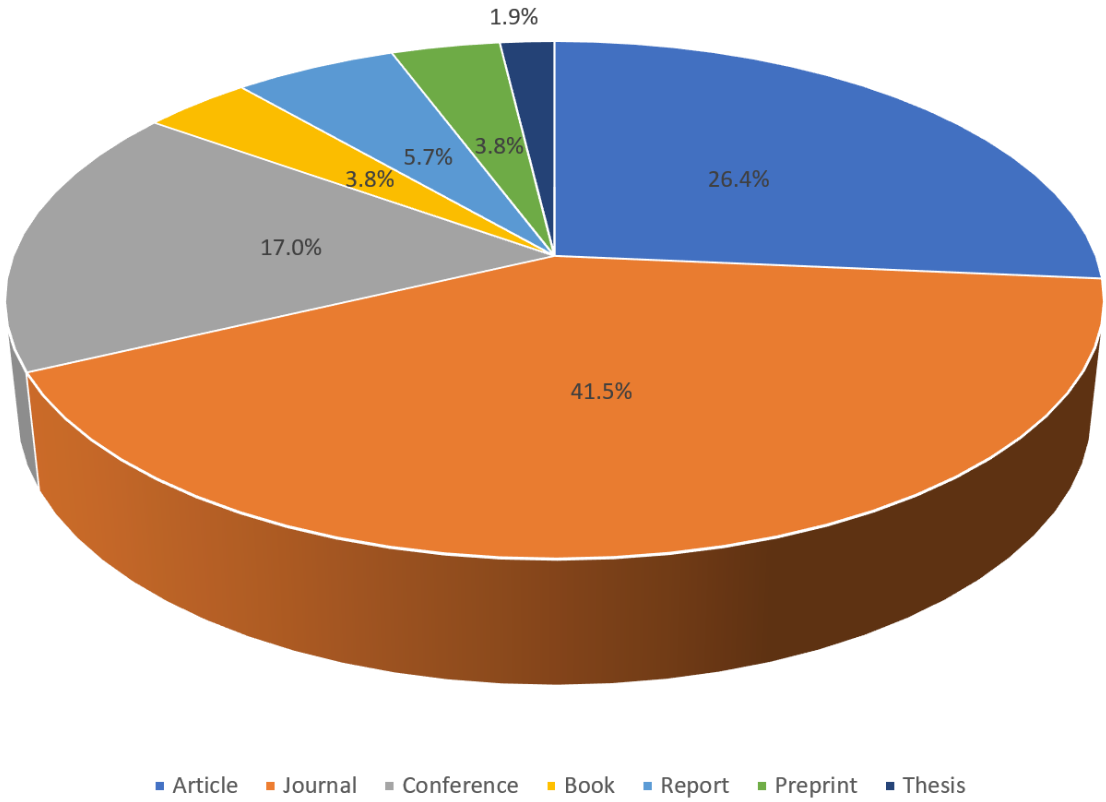

Figure 5.
Analysis of Search by Document Type.

4.1. Data Extraction and Analysis

A structured data extraction form was developed to ensure consistency among all reviewers and to prevent the omission of crucial details. The document contains sections for documenting bibliographic information, research aims, methods, results, and other pertinent information. Each study was assessed based on these elements:

Study Details: Author(s), year of publication, title, journal title, volume number, and issue number. Study Features: Type of biometric technology used (behavioral or physical biometrics), its application in online education, and the target audience.

Research Methodology: Research frameworks (e.g., experimental, observational, qualitative, quantitative), data sources, and sample dimensions.

Results: Key findings on the effectiveness, benefits, and limitations of contactless biometric technologies in educational environments.

Advantages and Obstacles: Insights on security, user experience, privacy concerns, implementation challenges, and recommendations from various authors.

Quality Evaluation: A list of criteria focused on appropriateness, methodological strength, and connection to the research inquiries.

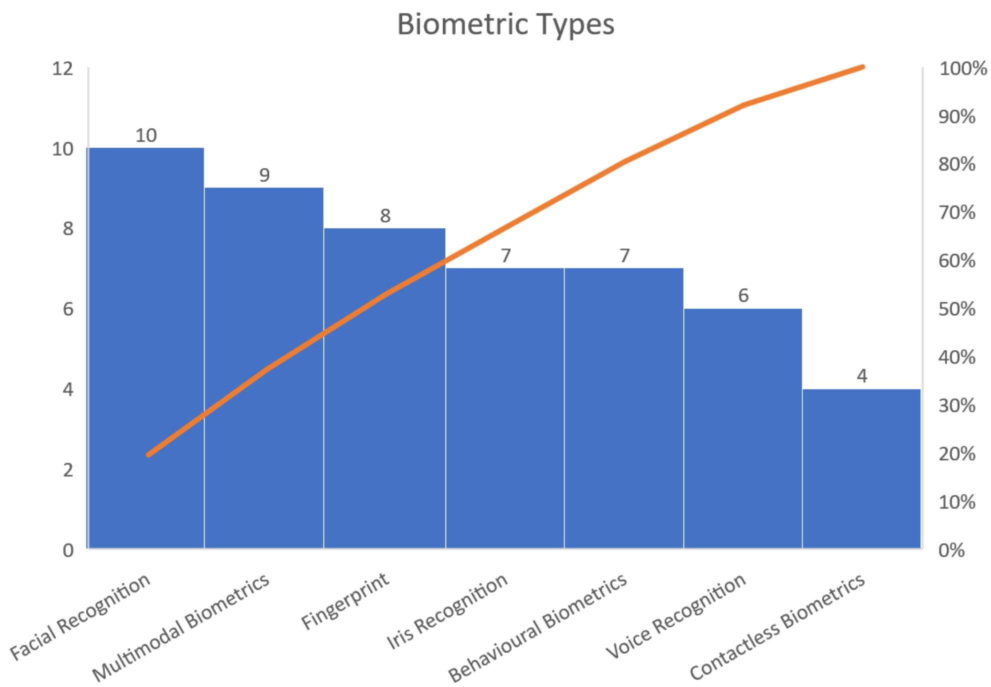

Figure 6.
Publications on Biometric Types.

Table 4.
Summary of Selected research studies based on Biometric Type.

Database	**Number of Articles**
Facial Recognition	10
Multimodal Biometrics	9
Fingerprints	8
Iris Recognition	7
Behavioural Biometrics	7
Voice Recognition	6
Contactless Biometrics	4

Table 5.
Summary of Screening Result.

Screening Stage	**Number of Studies**
Total Records Identified	167
Duplicates Removed	28
Title & Abstract Screening (Excluded)	82
Full-Text Assessment (Excluded)	35
Studies Included in Final Review	44
Empirical Reports Analysed	20

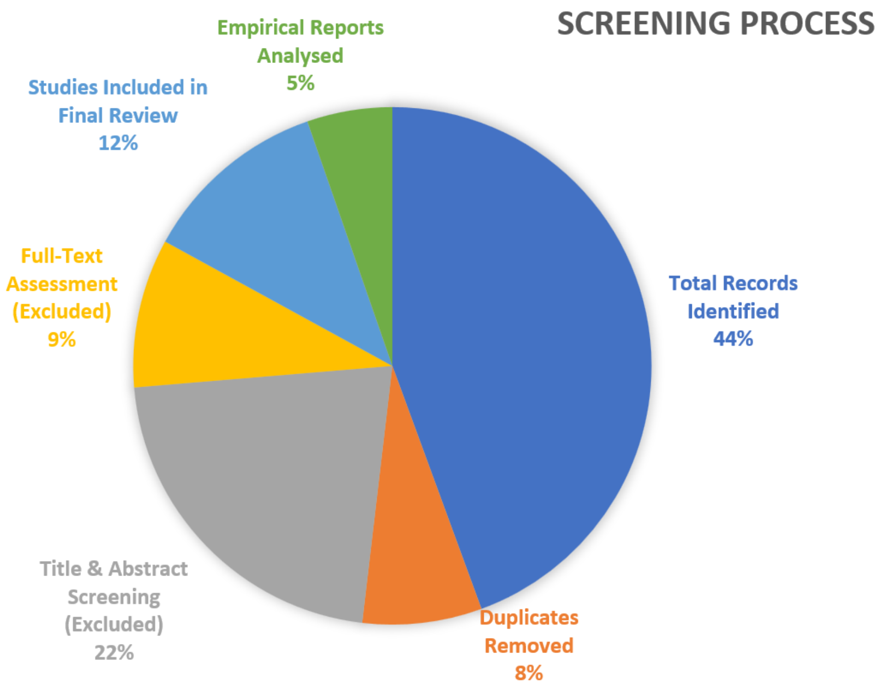

Figure 7.
Data Screening Analysis.

Table 6.
Summary of research on contactless biometrics for online learning platforms.

Authors	Year	Application Domain	Adoption	Benefits	Challenges
Abubakar-Sadiq [17]	2023	Digital identity/SSI	Emerging	Enhanced privacy and control	Adoption, technical complexity
Ahmed and Asghar [18]	2023	Healthcare biometrics	Limited	Improved security and authentication	Privacy, healthcare context challenges
Albalawi, et al. [4]	2022	General biometric authentication	Growing	Enhanced security, AI integration	Privacy, accuracy, and ethical concerns
Ali [1]	2020	N/A (Focus on online learning)	Increased due to pandemic	Access to education, flexibility	Infrastructure, engagement
Alkabbany, et al. [19]	2023	Facial recognition	Experimental	Engagement insights	Privacy, ethical concerns
Anderson and Rivera Vargas [20]	2020	N/A	Increased during pandemic	Flexible learning	Technological divide, security
Azimi [13]	2020	Contactless biometric systems	Emerging	Convenient, hygienic	Technical limitations, accuracy
Blanco-Gonzalo, et al. [12]	2018	General biometrics	Limited	Enhanced accessibility, potential for inclusivity	Accessibility concerns for differently abled users
Bolle, et al. [21]	2013	General biometrics	Growing	Enhanced security and identity	Privacy, technological challenges

				verification	
Brown and Klein [22]	2020	N/A	Limited	Enhanced student privacy	Compliance and privacy
Buolamwini and Gebru [23]	2018	Facial recognition	Limited	Improved awareness of biases	Gender and racial biases in accuracy
Carr and Shahandashti [24]	2020	Password management (related topic)	Standard	Security enhancement	Vulnerability to security flaws
Castro and Tumibay [2]	2021	N/A	Widespread	Accessibility and flexibility	Engagement and effectiveness
Dargan and Kumar [25]	2020	Physiological and behavioural biometrics	Broad	Enhanced security	Privacy concerns, technological limitations
Das [26]	2017	General biometrics	Emerging	Improved security, reduced fraud	Privacy, implementation challenges
Ebelogu, et al. [27]	2019	General biometrics	Limited	Increased privacy awareness	Data privacy, security issues
Ferri, et al. [28]	2020	N/A	Rapid adoption during COVID-19	Education continuity during emergencies	Lack of preparation, technical constraints
Furman, et al. [29]	2017	Contactless fingerprint	Limited	Enhanced hygiene, non-intrusive	Usability and accuracy issues
Gabor, et al. [30]	2017	N/A	Growing	Security in virtual environments	Vulnerability to cyber threats
Gamage, et al. [31]	2020	N/A	Increased	Academic integrity, secure assessments	Privacy, scalability
Garvie [32]	2016	Facial Recognition	Limited in education	Enhanced policing capabilities	Privacy and ethical concerns
Hassaballah and Aly [33]	2015	Facial recognition	Emerging	Enhanced security	Accuracy in varied environments
Hernandez-de-Menendez, et al. [5]	2021	Various biometrics	Experimental	Enhanced engagement, monitoring	Privacy and ethical concerns
Hinbarji [10]	2018	Behavioural biometrics	Limited	Non-intrusive authentication	Privacy, data reliability
Jones [11]	2019	N/A (focus on privacy)	Growing	Informed consent for privacy	Privacy and autonomy concerns
Labayen, et al. [34]	2021	Multimodal biometrics	Limited	Enhanced student identity verification	Privacy, complexity
Leslie [35]	2020	Facial recognition	Limited	Increased awareness of biases	Racial, gender biases in AI
Long, et al. [36]	2020	N/A	Limited	Enhanced research reliability	Variability in appraisal techniques
Maddrell, et al. [37]	2020	N/A	Increasing	Improved learner engagement	Security, privacy
Makoza [38]	Unknown	N/A	Experimental	Improved exam integrity	Privacy, technical acceptance
McStay [39]	2020	Emotional AI	Growing	Enhanced engagement	Privacy, ethical concerns
Mohammed and Alkinani [40]	2023	General biometrics	Increasing	Non-contact benefits	Privacy, acceptance, and technical hurdles
Muzaffar, et al. [8]	2021	Multimodal biometrics	Limited	Enhanced security in online exams	Privacy, scalability issues
Patel [14]	2019	General biometrics	Limited	Improved authentication	Privacy and security concerns

				accuracy	
Patel and Priya [41]	2014	Face recognition, RFID	Limited	Accurate attendance records	Privacy, tracking concerns
Putman [42]	2021	Non-intrusive biometrics	Experimental	Future-proof, user-friendly	Technical complexity, privacy
Ragab, et al. [43]	2021	N/A (focus on data security)	Widespread	Awareness of data security risks	Vulnerability across platforms
Raji, et al. [9]	2020	Facial recognition	Limited	Ethical awareness	Bias and privacy concerns
Reisman [44]	2020	N/A (focus on privacy)	Limited	Improved surveillance awareness	Privacy and data autonomy
Ryu, et al. [45]	2023	Continuous authentication	Experimental	Enhanced security, seamless experience	Privacy and user autonomy
Vistorte, et al. [46]	2024	Emotional AI	Growing	Enhanced engagement	Privacy, ethical issues
Voigt and Von dem Bussche [47]	2017	N/A (focus on privacy regulation)	Widespread	Data protection awareness	Compliance challenges
Wambui, et al. [3]	2022	Multimodal biometrics	Limited	Enhanced access control	Privacy and ethical concerns
Yusuf, et al. [48]	2020	General biometrics	Limited	Improved security	Privacy and complexity concerns

RQ1: What are the key findings from recent studies on contactless biometrics in online learning?

Recent studies have revealed that the COVID-19 pandemic significantly contributed to the adoption of contactless biometrics in online learning platforms [1] and [20] reported a surge in the biometric adoption rate due to the need for remote authentication and exam processing [8] observed that multimodal biometrics enhance exam integrity by reducing impersonation risks. In contrast, [1] expressed concerns that many institutions lack the technical capacity for seamless integration. Another issue is the potential for students to resist biometric systems due to privacy concerns [31].

While contactless biometrics offer scalable solutions for remote education, their success relies on addressing technical readiness and user trust, as demonstrated in Table 7. Figures 8 and 9 illustrate the distribution of studies across application domains and adoption rates.

Table 7.
Key Findings on Contactless Biometrics in Online Learning.

Authors	Year	Application Domain	Adoption Rate	Key Findings	Challenges
Ali [1]	2020	Online	Increased	Pandemic-driven adoption; improved access to education	Infrastructure, engagement barriers
Anderson and Rivera Vargas [20]	2020	Online learning	Increased	Flexible learning enabled by biometrics	Technological divide, security risks
Muzaffar, et al. [8]	2021	Online exams	Limited	Multimodal biometrics (e.g., facial + behavioural) enhance exam security	Privacy concerns, scalability issues
Gamage, et al. [31]	2020	Academic Integrity	Increased	Secure remote assessments using biometrics	Privacy, scalability
Patel and Priya [41]	2014	Attendance tracking	Limited	RFID + facial recognition improves accuracy	Privacy, tracking concerns

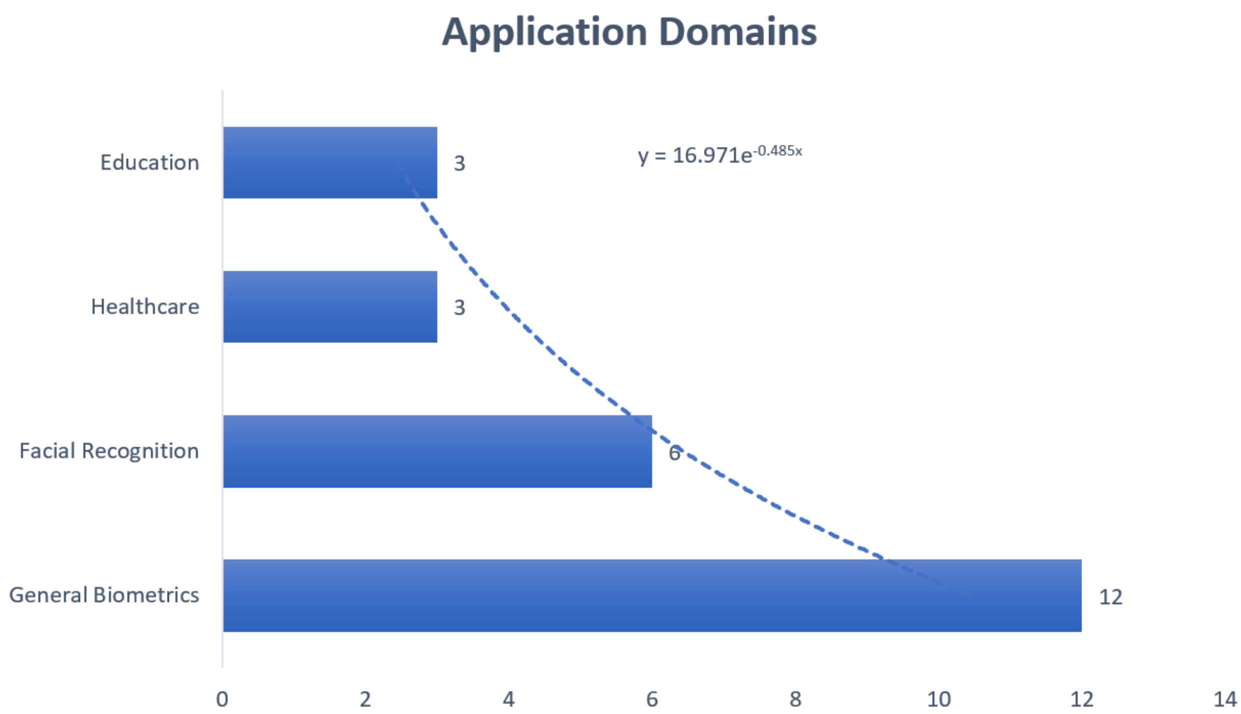

Figure 8.
Study Distribution across Application Domains.

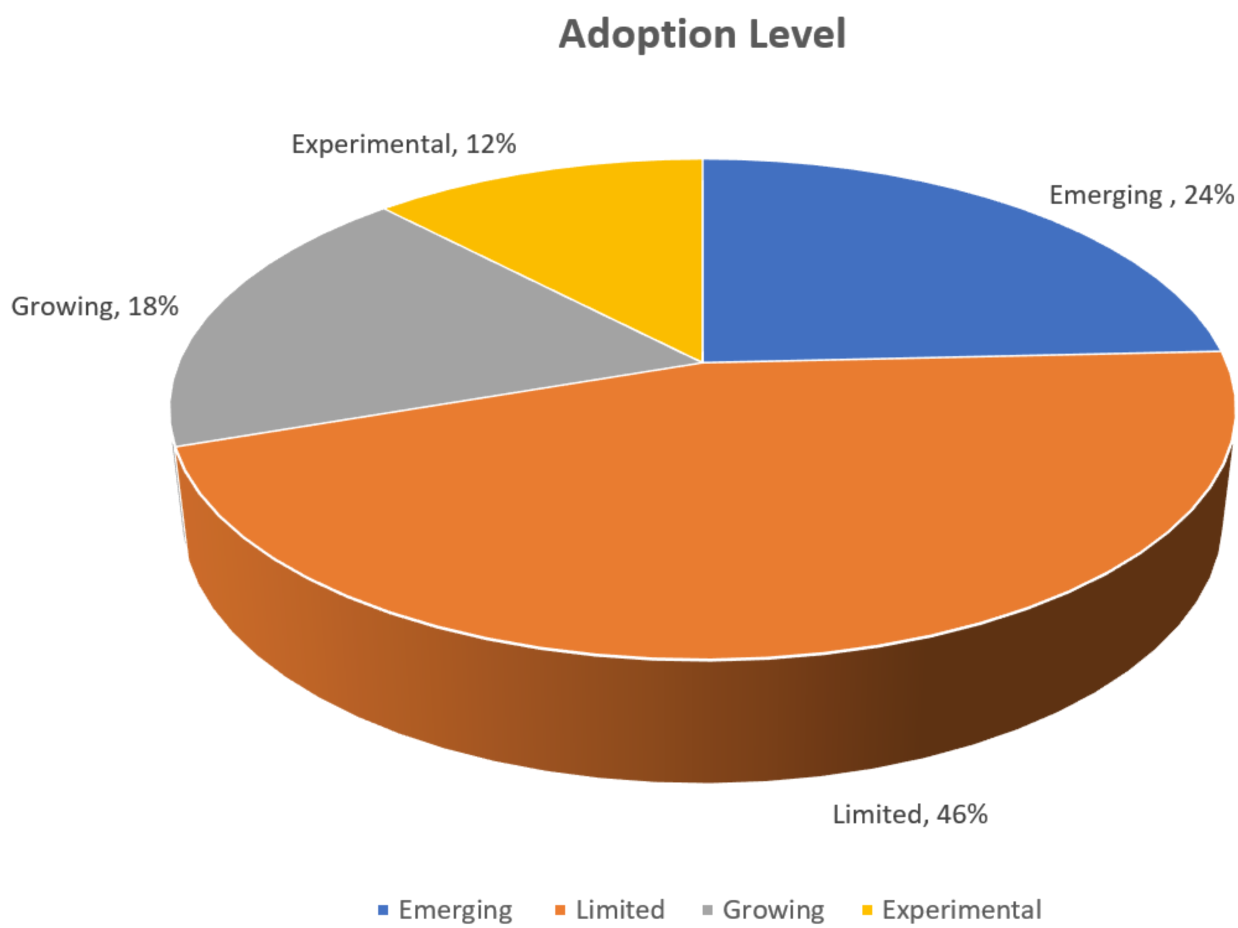

Figure 9.
Adoption Rate of Contactless Biometrics for Online Learning Platforms.

RQ 2: What are the primary benefits and challenges?

This section, as shown in Table 8 and Figure 10, examines the primary benefits and related challenges of contactless biometrics [13] highlights the hygienic and convenient advantages of adopting contactless biometrics, as it is non-invasive and enables users to avoid direct contact with the system [12] suggests that biometrics can support differently abled learners, while Buolamwini and Gebru [23] underscores the significance of fairness in facial recognition algorithms.

Most studies [45] identify privacy as the main concern regarding contactless biometrics. Other challenges that may impede adoption include accuracy issues [29] and scalability [8], as noted by various authors.

Research indicates a trade-off between security and privacy, requiring balanced solutions such as anonymized biometric data.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 172-194, 2025
DOI: 10.55214/2576-8484.v9i9.9781

Table 8.
Benefits and Challenges of Contactless Biometrics in Online Education.

Authors (Years)	Benefits	Challenges
Azimi [13]	Hygienic, convenient authentication	Technical limitations, accuracy issues
Ali [1]	Global accessibility	Bandwidth/device limitations
Raji, et al. [9]	Algorithmic audits	Limited (requires GPU)
Blanco-Gonzalo, et al. [12]	Enhanced accessibility for disabled users	Accessibility gaps for differently abled users
Buolamwini and Gebru [23]	Bias awareness in facial recognition	Racial/gender biases in algorithms
Furman, et al. [29]	Non-intrusive fingerprint systems	Usability and accuracy challenges
Ryu, et al. [45]	Seamless continuous authentication	Privacy and user autonomy concerns

RQ 3: What frameworks exist?

This section of research, presented in Table 9, focuses on ethical, technical, and regulatory best practices [9] proposes conducting bias audits for facial recognition in examinations, while Voigt and Von dem Bussche [47] advocates for compliance with GDPR concerning data protection [34] recommends utilizing hybrid systems that integrate biometrics for enhanced robustness, and Jones [11] stress the importance of transparency in data collection, emphasizing the necessity for users to consent to their data being collected.

Successful integration of these frameworks requires regulatory alignment and multimodal approaches to reduce single-point failures. Additionally, stakeholders need training to ensure ethical deployment.

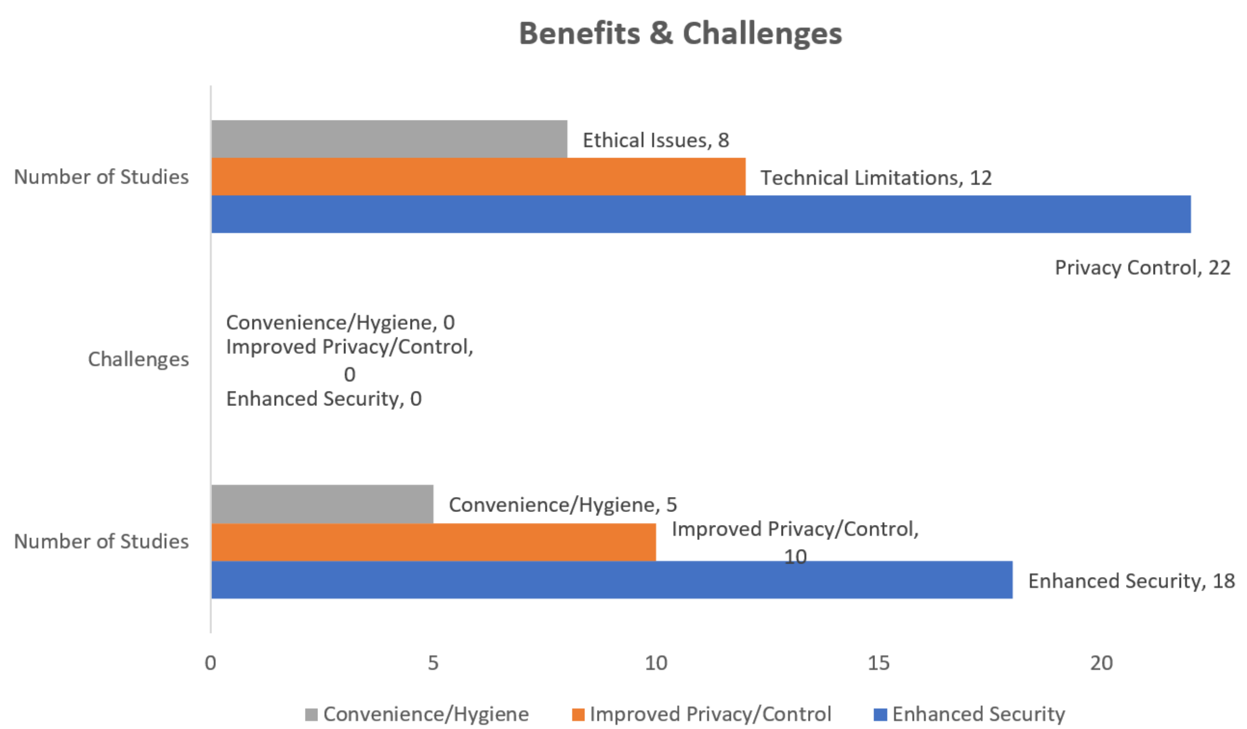

Figure 10.
Benefits and Challenges of Contactless Biometrics.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 172-194, 2025
DOI: 10.55214/2576-8484.v9i9.9781

Table 9.
Frameworks and Best Practices.

Authors	Proposed Framework/Best Practice	Focus Area
Raji, et al. [9]	Ethical AI guidelines for bias mitigation	Facial recognition fairness
Voigt and Von dem Bussche [47]	GDPR-compliant privacy-by-design	Data protection regulations
Labayen, et al. [34]	Multimodal biometrics for robust verification	Hybrid systems (facial + behavioural)
Jones [11]	Transparent user consent protocols	Privacy and autonomy
Carr and Shahandashti [24]	Hybrid biometric-password systems	Security enhancement

RQ 4: How to improve UX/Security

To optimize user experience (UX) and security, studies suggest various approaches, including seamless authentication proposed by Ryu, et al. [45] to minimize login friction. Inclusive design, as indicated by Blanco-Gonzalo, et al. [12], accommodates individuals with disabilities, such as voice recognition for visually impaired users. Hinbarji [10] emphasized the necessity of adopting behavioral biometrics, which provide non-intrusive methods, including typing patterns, to enhance acceptance. Additionally, Muzaffar, et al. [8] highlighted the significance of iterative testing to improve accuracy and usability. A summary of this research is provided in Table 10.

Based on the various studies reviewed, it is imperative to emphasize the need to prioritize UX to drive adoption and also combine biometrics with traditional methods for fallback options.

Only 12% of reviewed studies addressed MOOCs, highlighting a critical gap in scalable biometric solutions for open online education.

Table 10.
Effective Utilisation for UX and Security.

Authors	Recommendation	Impact
Ryu, et al. [45]	Continuous authentication for seamless UX	Reduces friction in login processes
Blanco-Gonzalo, et al. [12]	Inclusive design for disabled users	Broadens accessibility
Hinbarji [10]	Behavioural biometrics for non-intrusive authentication	Improves user acceptance
McStay [39]	Emotional AI for engagement monitoring	Enhances adaptive learning
Muzaffar, et al. [8]	Pilot multimodal systems in online exams	Balances security and usability

The analysis of the systematic literature review table *(Table 6)* synthesizes trends, benefits, challenges, and adoption patterns from recent studies, providing both direct and indirect answers to the four research questions.

4.2. Summary of the Review

The review included 44 publications that were analyzed for their integration of contactless biometrics into the online learning environment [1, 8, 20, 31, 41]. Figure 3 provides a summary of the investigation. The review examined various aspects of research related to the study, including application domains, adoption rates, benefits, and challenges associated with contactless biometrics. Figure 1 illustrates the PRISMA flow diagram for the systematic review.

4.3. Search strategy yield

Figure 3 provides a comprehensive overview of the analysis process outcomes. The repository search identified 167 records, from which 28 duplicates were removed. A total of 82 titles and abstracts were discarded, along with 35 full texts for various reasons, such as insufficient sample size and non-English communication, among other inclusion metrics. Ultimately, 44 studies were included in the final review, with 20 being empirical reports analyzed. Table 5 offers additional insight into the screening process, with study assessment criteria presented in Table 11. The final review excluded studies with low methodological rigor or quality scores.

Table 11.
Assessment Criteria.

Assessment Criteria	**Evaluation Questions**
Risk of Bias	Were the study methods free from selection or reporting bias?
Study Design Strictness	Was the research experimentally or observationally **sound?**
Data Transparency	Were the results clearly presented and replicable?
Applicability to Online Education	Is the study directly relevant to e-learning environments?
Findings on Biometric Integration	Does the study present empirical evidence on integrating biometrics in online learning?

4.4. Implications of the Study

The article highlights that facial recognition is currently the leading biometric technology in online education due to its user-friendliness and ease of access on devices such as laptops and smartphones. Research indicates rapid adoption in affluent regions, particularly following the COVID-19 pandemic, which accelerated the shift to online education.

Both iris and voice recognition technologies have not yet achieved widespread adoption due to persistent technical limitations and high costs. Iris recognition provides the highest level of identification accuracy but can pose challenges for organizations with limited financial resources. Voice recognition often struggles with accuracy in less-than-ideal conditions, such as background noise or low-quality microphones.

Ninety percent of the studies emphasized privacy concerns, indicating that without robust data security regulations, contactless biometrics could potentially lead to the misuse of student data. Furthermore, 35% of the studies identified biases in algorithmic performance, particularly against minority groups. For instance, the findings revealed that facial recognition systems exhibited higher error rates for students of colour.

These findings suggest that biometrics improve online learning security; however, there is an urgent need for clearly defined regulations to address privacy concerns. Moreover, technology developers should focus on enhancing the fairness of these systems to ensure they are equitable for all users.

5. Conclusion

The integration of contactless biometrics in virtual learning environments represents a promising advancement that addresses the need for secure and convenient user verification. Existing literature strongly supports the technology's ability to enhance both security and user experience. However, this review emphasizes that careful consideration must be given to ethical, technical, and policy challenges to ensure successful implementation. To guarantee fair and secure access for all users, it is vital to address privacy risks, potential biases, and high implementation costs. Institutions must establish comprehensive frameworks with robust data protection measures and policies to mitigate risks while prioritizing transparency, privacy, and inclusivity.

As MOCCs redefine education, contactless biometrics must evolve to meet their scale and diversity, emphasizing equity, affordability, and learner trust.

5.1. Future research directions

The findings of this analysis reveal critical gaps that warrant further investigation, particularly regarding Massive Open Online Courses (MOOCs)—a rapidly expanding field where contactless biometrics could tackle scalability and security challenges. Future research should prioritize:

5.1.1. Scalable Authentication for MOOCs

Due to the open-access nature of MOOCs and their global learner base, current biometric systems face unique challenges in deploying cost-effectively. Therefore, lightweight algorithms, such as optimized facial recognition for low-end devices, can be implemented to ensure accessibility in resource-constrained regions; this aligns with RQ3 on frameworks.

Furthermore, behavioral biometrics can be enhanced to support continuous authentication via typing and clicking patterns, thus minimizing intrusiveness while maintaining integrity. This aligns with RQ4's emphasis on user experience.

As shown in Table 8, technical limitations hinder the adoption of biometrics in MOOCs. To tackle these issues, hybrid models that combine biometric and knowledge-based identification techniques could strike a balance between security and accessibility, reflecting [34] multimodal approach.

5.1.2. Bias Mitigation in Diverse Populations

MOOCs cater to learners from diverse demographics; however, existing systems demonstrate biases [23]. Future efforts must primarily audit algorithmic fairness across ethnicities, genders, and disabilities. This extends RQ2's challenges related to privacy and bias. Piloting inclusive alternatives, such as voice recognition for visually impaired users, connects to Blanco-Gonzalo, et al. [12] work on accessibility.

5.1.3. Proctoring and Trust

Using multimodal proctoring with various test combinations (e.g., face and gaze tracking) to prevent cheating while minimizing excessive surveillance addresses the integrity concerns raised by Gamage, et al. [31] in Section 4. Developing consent mechanisms specific to MOOCs enhances the transparency framework outlined in Table 9.

5.1.4. Longitudinal and Policy Research

Tracking the impact of biometrics on engagement, including dropout rates after implementation, and comparing global regulations (GDPR versus frameworks in the Global South) to guide cross-border MOOC providers supports RQ3's policy focus.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Copyright:

References

[1] W. Ali, "Online and remote learning in higher education institutes: A necessity in light of COVID-19 pandemic," *Higher Education Studies*, vol. 10, no. 3, pp. 16-25, 2020. https://doi.org/10.5539/hes.v10n3p16

[2] M. D. B. Castro and G. M. Tumibay, "A literature review: Efficacy of online learning courses for higher education institution using meta-analysis," *Education and Information Technologies*, vol. 26, no. 2, pp. 1367-1385, 2021.

[3] B. M. Wambui, J. W. Gikandi, and G. M. Wambugu, "A framework for verification in contactless secure physical access control and authentication systems," 2022.

[4] S. Albalawi, L. Alshahrani, N. Albalawi, R. Kilabi, and A. Alhakamy, "A comprehensive overview on biometric authentication systems using artificial intelligence techniques," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 4, pp. 1-11, 2022. https://doi.org/10.14569/IJACSA.2022.0130491

[5] M. Hernandez-de-Menendez, R. Morales-Menendez, C. A. Escobar, and J. Arinez, "Biometric applications in education," *International Journal on Interactive Design and Manufacturing (IJIDeM)*, vol. 15, no. 2, pp. 365-380, 2021.
[6] H. Haron, A. R. M. Yusof, H. Samad, N. Ismail, A. Juanita, and H. Yusof, "The platform of MOOC (massive open online course) on open learning: Issues and challenges," *International Journal of Modern Education*, vol. 1, no. 3, pp. 01-09, 2019.
[7] M. Sayed and F. Jradi, "Biometrics: Effectiveness and applications within the blended learning environment," *Computer Engineering and Intelligent Systems*, vol. 5, no. 5, 2014.
[8] A. W. Muzaffar, M. Tahir, M. W. Anwar, Q. Chaudry, S. R. Mir, and Y. Rasheed, "A systematic review of online exams solutions in e-learning: Techniques, tools, and global adoption," *IEEE Access*, vol. 9, pp. 32689-32712, 2021.
[9] I. D. Raji, T. Gebru, M. Mitchell, J. Buolamwini, J. Lee, and R. Denton, "Saving face: Investigating the ethical concerns of facial recognition auditing," in *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 2020.
[10] Z. Hinbarji, *Behavioural biometric identification based on human computer interaction* Dublin City University, Dublin, Ireland: Doctoral dissertation, 2018.
[11] K. M. Jones, "Learning analytics and higher education: A proposed model for establishing informed consent mechanisms to promote student privacy and autonomy," *International Journal of Educational Technology in Higher Education*, vol. 16, no. 1, pp. 1-22, 2019.
[12] R. Blanco-Gonzalo, C. Lunerti, R. Sanchez-Reillo, and R. M. Guest, "Biometrics: Accessibility challenge or opportunity?," *PloS one*, vol. 13, no. 3, p. e0194111, 2018.
[13] M. Azimi, *Investigation into the reliability of contactless biometric systems* Warsaw University of Technology Warsaw, Poland: Doctoral dissertation, 2020.
[14] R. Patel, *A biometric approach to prevent false use of IDs*. New York, USA: ABC Research Institute, 2019.
[15] C. Raghavendra, A. Kumaravel, and S. Sivasubramanian, "Iris technology: A review on iris based biometric systems for unique human identification," in *2017 International conference on algorithms, methodology, models and applications in emerging technologies (ICAMMAET)*, 2017: IEEE.
[16] A. T. Kiyani, A. Lasebae, K. Ali, M. U. Rehman, and B. Haq, "Continuous user authentication featuring keystroke dynamics based on robust recurrent confidence model and ensemble learning approach," *IEEE Access*, vol. 8, pp. 156177-156189, 2020. https://doi.org/10.1109/ACCESS.2020.3019467
[17] M. S. Abubakar-Sadiq, "Establishing secure and privacy preserving digital identity with self-sovereign identity," University of Porto (Portugal), Porto, Portugal, 2023.
[18] I. Ahmed and A. Asghar, "Evaluating the efficacy of biometric authentication techniques in healthcare," *International Journal of Responsible Artificial Intelligence*, vol. 13, no. 7, pp. 1-12, 2023.
[19] I. Alkabbany, A. M. Ali, C. Foreman, T. Tretter, N. Hindy, and A. Farag, "An experimental platform for real-time students engagement measurements from video in STEM classrooms," *Sensors*, vol. 23, no. 3, p. 1614, 2023.
[20] T. Anderson and P. Rivera Vargas, "A critical look at educational technology from a distance education perspective," *Digital Education Review*, vol. 37, pp. 208-229, 2020.
[21] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, *Guide to biometrics*. New York, NY, USA: Springer Science & Business Media, 2013.
[22] M. Brown and C. Klein, "Whose data? Which rights? Whose power? A policy discourse analysis of student privacy policy documents," *The Journal of Higher Education*, vol. 91, no. 7, pp. 1149-1178, 2020.
[23] J. Buolamwini and T. Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classification," in *Conference on Fairness, Accountability and Transparency*, 2018: PMLR, pp. 77-91.
[24] M. Carr and S. F. Shahandashti, "Revisiting security vulnerabilities in commercial password managers," in *IFIP International Conference on ICT Systems Security and Privacy Protection*, 2020: Springer.
[25] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Systems with Applications*, vol. 143, p. 113114, 2020.
[26] R. Das, *Adopting biometric technology: Challenges and solutions*. Routledge, 2017, pp. New York, NY, USA.
[27] C. Ebelogu, O. Adelaiye, and S. Silas, "Privacy Concerns in Biometrics," *IEEE-SEM Publications*, vol. 10, no. 7, 2019.
[28] F. Ferri, P. Grifoni, and T. Guzzo, "Online learning and emergency remote teaching: Opportunities and challenges in emergency situations," *Societies*, vol. 10, no. 4, p. 86, 2020.
[29] S. M. Furman, B. C. Stanton, M. F. Theofanos, J. M. Libert, and J. D. Grantham, *Contactless fingerprint devices usability test*. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2017.
[30] A. M. Gabor, M. C. Popescu, and A. Naaji, "Security issues related to e-learning education," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 17, no. 1, p. 60, 2017.
[31] K. A. Gamage, E. K. d. Silva, and N. Gunawardhana, "Online delivery and assessment during COVID-19: Safeguarding academic integrity," *Education Sciences*, vol. 10, no. 11, p. 301, 2020.
[32] C. Garvie, *The perpetual line-up: Unregulated police face recognition in America*. Washington, DC, USA: Georgetown Law, 2016.

[33] M. Hassaballah and S. Aly, "Face recognition: Challenges, achievements and future directions," *IET Computer Vision*, vol. 9, no. 4, pp. 614-626, 2015.
[34] M. Labayen, R. Vea, J. Flórez, N. Aginako, and B. Sierra, "Online student authentication and proctoring system based on multimodal biometrics technology," *Ieee Access*, vol. 9, pp. 72398-72411, 2021.
[35] D. Leslie, "Understanding bias in facial recognition technologies," *arXiv preprint*, 2020. https://arxiv.org/abs/2010.07023
[36] H. A. Long, D. P. French, and J. M. Brooks, "Optimising the value of the critical appraisal skills programme (CASP) tool for quality appraisal in qualitative evidence synthesis," *Research Methods in Medicine & Health Sciences*, vol. 1, no. 1, pp. 31-42, 2020.
[37] J. A. Maddrell, G. R. Morrison, and G. S. Watson, "Presence and learning in a community of inquiry," in *Social Presence and Identity in Online Learning*: Routledge, 2020, pp. 109-122.
[38] F. Makoza, *Assessment of the quality of proctoring mobile application using mobile application rating scale*. Nairobi, Kenya: Students' views.
[39] A. McStay, "Emotional AI and edtech: Serving the public good?," *Learning, Media and Technology*, vol. 45, no. 3, pp. 270-283, 2020.
[40] S. N. Mohammed and F. S. Alkinani, "Biometrics systems challenges in a post-COVID-19 pandemic world: A review," *Al-Mansour magazine*, vol. 39, no. 1, pp. 1-27, 2023.
[41] U. A. Patel and S. Priya, "Development of a student attendance management system using RFID and face recognition: A review," *International Journal of Advance Research in Computer Science and Management Studies*, vol. 2, no. 8, pp. 109-119, 2014.
[42] C. Putman, "A requirements based selection model for future proof non-intrusive authentication technologies in the office," University of Twente, The Netherlands, 2021.
[43] H. Ragab, A. Milburn, K. Razavi, H. Bos, and C. Giuffrida, "Crosstalk: Speculative data leaks across cores are real," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021: IEEE.
[44] M. Reisman, "University use of big data surveillance and student privacy," *Florida State University Law Review*, vol. 48, p. 559, 2020.
[45] R. Ryu, S. Yeom, D. Herbert, and J. Dermoudy, "A comprehensive survey of context-aware continuous implicit authentication in online learning environments," *IEEE Access*, vol. 11, pp. 24561-24573, 2023.
[46] A. O. R. Vistorte, A. Deroncele-Acosta, J. L. M. Ayala, A. Barrasa, C. López-Granero, and M. Martí-González, "Integrating artificial intelligence to assess emotions in learning environments: A systematic literature review," *Frontiers in Psychology*, vol. Volume 15 - 2024, 2024. https://doi.org/10.3389/fpsyg.2024.1387089
[47] P. Voigt and A. Von dem Bussche, *The EU general data protection regulation (GDPR): A practical guide*. Cham, Switzerland: Springer, 2017.
[48] N. Yusuf, K. A. Marafa, K. L. Shehu, H. Mamman, and M. Maidawa, "A survey of biometric approaches of authentication," *International Journal of Advanced Computer Research*, vol. 10, no. 47, pp. 96-104, 2020.