Mesopotamian journal of Cybersecurity
Vol.5,No.2, **pp**. 319–336
DOI: https://doi.org/10.58496/MJCS/2025/020; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Integrating Law, Cybersecurity, and AI: Deep Learning for Securing Iris-Based Biometric Systems

Saif Alaa Hussein [1], Hasan Ali Al-Tameemi [2], Ghadeer Ghazi Shayea [2,3], Firas Jamal Shakir [4], Mohd Hazli Mohammed Zabil [3], Mustafa Abdulfattah Habeeb [5], Yahya Layth Khaleel [5, *]

[1] *College of Law, Imam Ja'afar Al-Sadiq University, Baghdad, 10001, Iraq.*
[2] *Technical College, Imam Ja'afar Al-Sadiq University, Baghdad, 10001, Iraq.*
[3] *College of Information Technology, Universiti Tenaga Nasional (UNITEN), 43000, Kajang, Selangor, Malaysia.*
[4] *Ministry of Defence, Iraq.*
[5] *College of Computer Science and Mathematics, Tikrit University, Iraq.*

ARTICLE INFO

Article History
Received 25 Mar 2025
Accepted 25 Apr 2025
Published 08 May 2025

Keywords
Biometric Authentication
Iris Recognition
Cybersecurity
Deep Learning
ResNet50
Data Protection
Law
Artificial Intelligence
Health-Aware Biometrics
Legal and Ethical Challenges

ABSTRACT

The increasing prevalence of biometric authentication systems as part of the organizational cybersecurity ecosystem highlights the need to gain further knowledge of both legal and technical considerations related to biometric data protection. The inherent nature of biometric data (unique to an individual and unchangeable) elicits a vulnerability to cyber abuse along with privacy risks. This study discussed the legal landscape regulating biometric data, underscoring our awareness of legislation inadequacies in regions of the world, with a specific reference to Iraq, and its comparison to international standards that employ laws (GDPR, EU AI Act). This study indicated that there is an urgency in establishing robust, effective, enforceable protections for biometric information from unauthorized collection and circumvention. In terms of cybersecurity practices, ensuring the integrity, confidentiality and availability of biometric data are key. When there are ineffective legal and regulatory measures, the risks of exposing sensitive data and forgetting biometric security have significant potential to degrade the effectiveness of biometric systems for secure authentication. This study suggests that technological innovations with integrated legal considerations will aid in the creation of legitimate biometric systems that can improve quality and security. In addition to the pressing legality themes, this study explores a practical illustration of deep learning through a ResNet50-based model to classify iris health conditions. The model for classifying an iris as "mature" or "immature" has the potential to ensure the reliability of authentic biometric systems, and the model has a validity score of 98%. This specific example presents the employability of AI in potentially advancing biometric security. This study explored ways to recognize the dual structure of legal impact and technological developments in this field to ultimately create a balance where biometric systems remain palatable and convey an ethical obligation.

1. INTRODUCTION

Biometric authentication is a key security measure of modern cybersecurity schemes, as it enables user identification and the confirmation of identity on the basis of unique physiological characteristics [1][2]. Biometric systems now appear to replace the typical password protection security mechanisms used today in all situations, including sensitive environments such as banking, governmental, healthcare, and corporate operations, where basic password protection concepts cannot address the advanced ongoing cyber attacks faced daily [3]. When considering biometrics, perhaps the highest valued modality is iris recognition, which enjoys widespread acceptance for eliminating forgery, has greater than 90% accuracy for real-world applications, and is stable over time, meaning that the patterns remain unchanged throughout an individual's life [4].

Despite their technical advantages, iris recognition systems may lead to unpleasant legal and cybersecurity concerns. Because biometric data are immutable in their legal frameworks, if an unauthorized entity acquires biometric data, it cannot

*Corresponding author. Email: yahya@tu.edu.iq

be changed such as security tokens or passwords [5]. The immutability of biometric data makes it appealing to cybercriminals for attack; therefore, we need a substantial legal framework in place for the collection, processing, and storage of biometric data [6], [7]. The worldwide law regarding biometric data use still remains limited and, at best, inconsistent and isolated in nature; thus, when looking at how additional jurisdictions address the challenges of biometric data use, the spectrum of laws ranges from not addressing biometric data at all to addressing issues in a manner that establishes uniformity [8], [9]. As examples of guidelines for biometric law have been developed across the globe, to date, the European Union has provided the most comprehensive regulation with the General Data Protection Regulation (GDPR) scheme [10], [11]. One tenet of the GDPR is that "biometric data is a special category of personal data" and requires additional safeguards when implemented [12]. Unfortunately, many other jurisdictions lack dedicated legislation for biometric data or have indefinite clauses and fall short of adequate protection from biometric data exploitation [13].

Currently, in Iraq, individuals are significantly exposed to privacy risks from artifacts in their biometric data because of a lack of well-defined legal statutes on what constitutes biometric data [14]. With no well-defined legal framework regarding biometric data, individuals potentially leave themselves vulnerable because there are no mandated consent procedures, rules around the encryption of data, or independent oversight to prevent organizations from misusing the data [15]. The shortcomings in legal defense and safeguarding for citizens can compromise their personal privacy and compromise or degrade the security of all forms of cybersecurity infrastructures that rely on biometric authentication [16]. While there is innovation in technology related to biometrics, it must align with legislation so that security and trust can be realized and maintained.

From the standpoint of cybersecurity and the protection of biometric data, this approach also means going beyond technical safeguards. The entire framework around privacy and security for biometric data must include legal safeguards and controls and ethical and procedural considerations [17]. The largest area of perceived misuse or threat to biometric authentication data is access or transferable value of the data, such as identity theft; unauthorized access to repositories that hold sensitive data; and social engineering of staff into disclosing data related to biological attributes by impersonating the user to access or redeem benefits they are entitled to [6]. The consequences of unauthorized biometric data breaches have a lasting impact on administrations, but the severity of consequences is dependent on the scope of the breach, such as the context of national security or healthcare, where the integrity of the data or level of control of access is premised [18].

On the other hand, iris recognition systems face challenges from the normal variability of biological attributes in terms of navigating health issues [19]. For example, the development of cataracts can dramatically change the functional visual attributes of the iris, leading to a higher false rejection (or acceptance) rate for a biometric system [20], [21]. This is mainly a technical problem but also explores various problems of a stakeholder, professional, and security nature for individuals and organizations whereby misidentification (false acceptance) affords access to unauthorized people, or false rejection denies payment to authorized personnel. There is a general point to be made here, which is that there is a need for biometric systems to be health aware in their functionality and to not only authenticate identity but also assess the health status (as related to the function of the biometric attribute) of the analyzed biometric attribute [22], [23].

In addition, Iris recognition systems have the potential for a very high level of security; however, every biometric is to be understood and to be operated on the premise that the iris is healthy [19], [24]. Traditional biometric systems do not consider health variability[133]. This potential for false acceptances or false rejections is heightened by the health-aware aspects of this biometric research, which we aim to include in the analysis, thus presenting a hole in the cyber security chain but also, if different forms of legal regulations do not assist in decreasing risk, biometric systems will continue to face crime [25], [26].

The research outlined here makes significant contributions to biometric security and deep learning research by providing a health-aware and operational understanding of iris recognition. In addition to the analysis using convolutional neural networks, specifically the ResNet50 architecture, we hope to add deficiencies but robustness to iris recognition systems to allow industries to use them with confidence. The inclusion of a health assessment increases the accuracy of biometric systems while also contributing to global cybersecurity objectives by reducing vulnerability concerning compromised biometric attributes due to medical health characteristics[134]. We will also imagine a more extensive examination of health-aware deep learning technology and more alignment with accepted practices regarding legal and ethical actions, thus helping to develop good biometric systems that are ii, secure, and compliant with current laws that conform to international standards.

This study provides the following contributions:

- This paper describes the gaps in legal frameworks to protect biometric data, particularly in underregulated settings such as Iraq.
- This study provides a comprehensive theory that relates biometric authentication with cybersecurity procedures, policies, compliance, and related data protection legislation.
- A ResNet50-based deep learning model that collects iris health classification data in the context of biometric authentication reliability evaluation and classification is provided.

- A health-aware biometric system that aims to minimize errors and compromised biometric traits, which leads to unintentional access, is introduced.
- Emphasizes the need for emerging technologies to marry ethical and legal dimensions.

The future of biometric cybersecurity is at a point where the abundance of digital opportunities will only continue to evolve and requires future legal actors to make increasingly complex decisions, in terms of balancing rigor, managing risk through law, and data protection laws, incorporating advanced AI-based models and using technology to create ethical and legally compliant, trustworthy biometric authentication systems in a world that tends to collapse privacy.

2. BIOMETRICS AND AI: SECURITY, LAW, AND EMERGING RISKS

This chapter reviews the current academic literature on biometrics, cybersecurity, artificial intelligence (AI), and law. It discusses biometric data as a technical, cybersecurity, legal, and ethical challenge. Furthermore, it examines how AI has improved biometric systems while simultaneously introducing new vulnerabilities, including the risk of adversarial attacks. Additionally, it explores various legislative frameworks regulating biometric data, presents real-world applications and associated risks, and offers recommendations for creating secure and reliable biometric systems (see Figure 1).

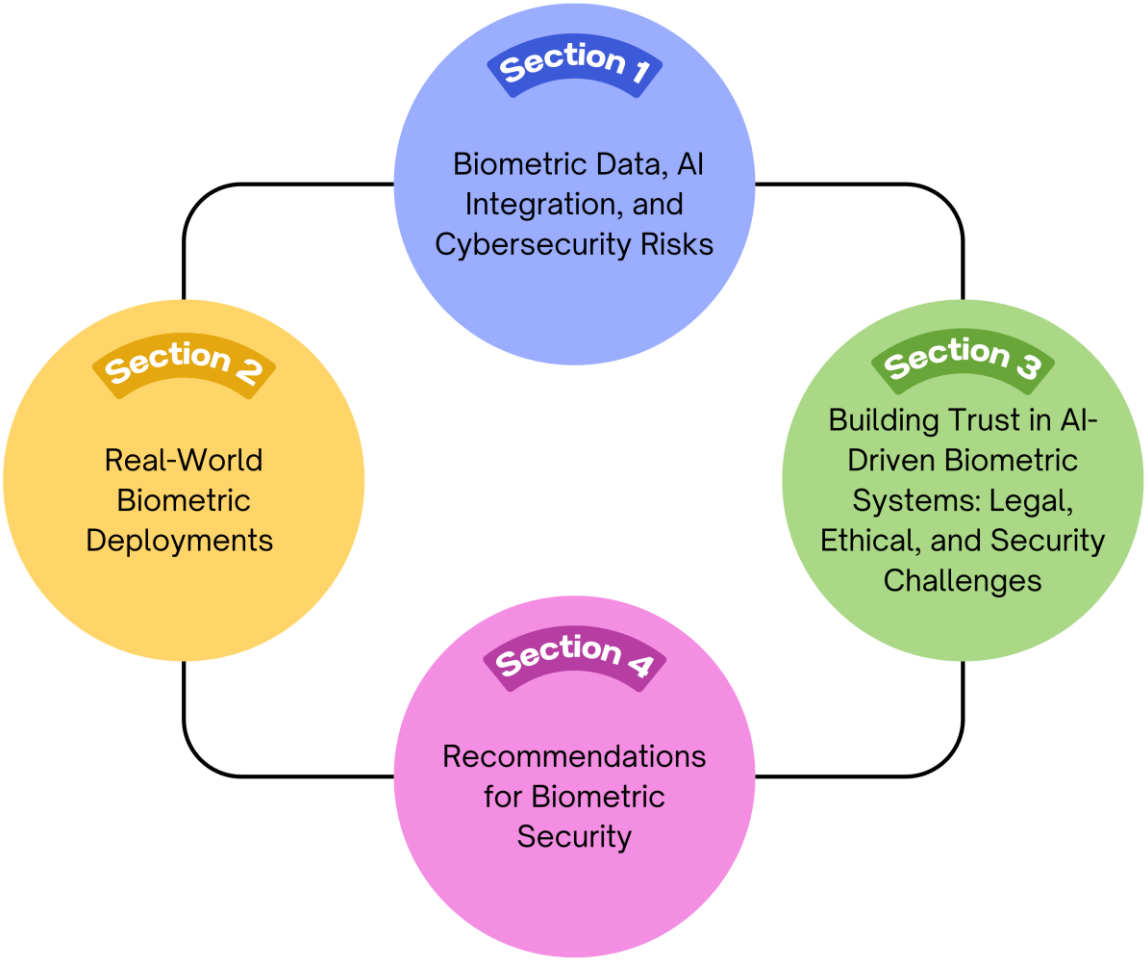

Fig. 1. Biometrics and AI

2.1. Biometric Data, AI Integration, and Cybersecurity Risks

The growth in the use of biometric data in workplaces for organizational and security purposes has created increased reliance on employee privacy rights [27], [28]. Examples of biometric traits, which can be physical [1], physiological [29], or behavioral [30], are fingerprints [31], facial characteristics [32], voice [33], and gait [34]. There is a need for a clearly defined statutory scheme regulating employee privacy to ensure data protection in the workplace [35]. Furthermore, the rapid emergence of artificial intelligence (AI) technologies used in workplaces introduces new difficulties for legal governance as well as cybersecurity infrastructures [36], [37].

Biometric data can be defined as personal data processed through technical means related to the physical, physiological, or behavioral characteristics of a person whothat can identify that individual uniquely [38], [39]. A few examples of biometric data include fingerprints, facial features, voice tone or sound, eye movement, contours of the body, gait, heart rate, blood pressure, and even smell. The types of biometric data are frequently deployed in workplaces to verify attendance and allow access to a secured area [40]–[43].

According to the European Union Artificial Intelligence Act [44], biometric data can be divided into two types:

- Biometric Recognition: Automatic identification on the basis of physical, physiological, and behavioral characteristics such as the movement of the eye and face, as well as voice [45]. The biometric data are compared to the individual's biometric data, which are matched against a reference database independent of consent but granted for the purpose of verifying identity.

- Biometric Classification: Listing individuals into categories or classes on the basis of their biometric data for subsequent predispositions (e.g., age, racial or ethnic origin, religion, political orientation, or sexual orientation) [46], [47]. This does not refer to filtration systems for commercial purposes, as with social media.

The 2024 EU Regulation describes an emotion recognition system as an AI-based system intended to detect or infer a person(s)' primary emotion (e.g., happiness, sadness, anger, and anxiety), as well as their intentions, on the basis of biometric data [48]. An emotion recognition system can be as follows:

- Real-time Systems: Data are captured and analyzed immediately after capture [49].
- Postrecorded Systems: Rely on prerecorded data (e.g., video footage) [50].

It is warned against the use of these systems in workplace or workplace environments without clear regulations because, when an unjust algorithm is used, AI systems unfairly affect decisions or evaluations involving employment and hiring. In addition, the security of biometric information is becoming an important part of legal and cybersecurity discussions [6]. Different jurisdictions have prepared for biometric data challenges to varying degrees that bobble legal maturity and enforcement [51]. An analysis of these legal frameworks will help elucidate how biometric data are treated in other legal systems; it will clarify the discrepancies in regulatory protection.

Emotion recognition systems should not be run in workplaces without clear regulation, as they could unwisely bias or make employment decisions or evaluations on the basis of criteria that may be biased and/or unverifiable algorithms [52]. Additionally, biometric data are considered one of the most sensitive data types because they are unique to individuals and cannot be changed [53]. Biometric data stand out as a target for cybersecurity threats. Cybersecurity includes protection from threats that target biometric data:

- Hacking or extortion [54].
- Identification Spoofing or social engineering attacks [55].
- Misuse in AI systems that are unregulated (i.e., if employees' fingerprints are leaked from an attendance database, then they could be used for identity theft or to breach otherwise confined internal systems) [45].

In Iraq, several other considerations include the following [56], [57]:

- No strong cybersecurity infrastructure.
- There are no national standards for data encryption or standards for testing systems.
- There is low coordination between bodies of law and bodies of a technical nature.

2.2. Real-world biometric deployments

The real-world use of biometric technologies in different parts of the globe has demonstrated both their potential advantages and very real dangers, especially when appropriate legal and ethical constructs are lacking [58], [59]. One significant case is Amazon, which, in 2020, was under substantial scrutiny for its use of facial recognition technologies—specifically, its own software "Rekognition"—to monitor employees going about their duties while in distribution warehouses [60]. The practice drew criticism from employee advocates over their perceived invasion of workers' privacy, as well as concerns related to the potential for discriminatory evaluations from biometric surveillance. Activism, led by civil rights organizations and other groups in the public interest, resulted in Amazon temporarily stopping using the technology until further clarity on the legal standing of biometric information could be established [61]. The Amazon example captured public attention while reinforcing the need for clear regulations and transparency regarding biometric monitoring in the workplace.

Another significant case is that of Clearview AI, which is a U.S. company that collects biometric information by scraping billions of facial images from several social media sources without consent from users [62]. The information was scraped to develop facial recognition capabilities to be sold as services to various law enforcement and private entities, resulting in many lawsuits in Europe and the United States. The European Union characterized these acts as clear violations of the General Data Protection Regulation (GDPR), as explicit consent is required to gather and use personal information [63]. The Clearview AI case has become an important reference point when discussing the dangers of the uncontrolled gathering

of biometric information and the urgency of establishing comprehensive and robust international regulations to control personal information data protection.

In the United Arab Emirates, airports such as Dubai International now have facial recognition systems in place to streamline the clearing process for passengers [64]. The use of these systems substantially increases passenger throughput, as they can pass through smart gates without lengthy identification checks [65]. Operationally beneficial as they are, the UAE's data protection laws permit significant exemptions for the government's use of biometric data, demonstrating a lack of accountability. Additionally, the absence of any transparency regarding what data are stored, or if any information sharing, aggregating or processing occurs by authorities, creates serious risks regarding individual privacy and data protection [66]–[68].

2.3. Building Trust in AI-Driven Biometric Systems: Legal, Ethical, and Security Challenges

Artificial intelligence (AI) refers to a branch of computer science that provides machines with the ability to replicate human intelligence processes [69], [70]. The simulation of processes such as learning, reasoning, problem-solving, and decision-making used to be the sole purview of human beings. AI has revolutionized countless elements of human experience and has blurred traditional boundaries between disciplines [71]–[75]. AI began in computer science and mathematics but has extended rapidly into many fields, including health care [71], [76], [77], finance [78], [79], education [80], [81], agriculture [82], [83], and environmental sciences [84], [85]. For example, AI has been used in health care to identify diseases with a high degree of accuracy and to assist doctors in the early identification of issues and personalization of treatment [86], [87]. In finance, AI is used to find fraud, optimize investment and automate complex thinking [88]. In agriculture, AI systems can analyze the health of a crop, predict yield and enhance sustainability in regard to food production [89]. In environmental science, AI has been used to model climate change and assist with disaster response [90]. These factors alone demonstrate the truly flexible capabilities of AI to create innovative thinking, efficiency, and completely new ways of understanding what is possible in these areas, among other areas.

As AI technology becomes more commonplace in a range of sectors, the integration of AI in legal and security frameworks becomes increasingly necessary [91], [92]. As new AI technology expands, we are confronted with difficult legal issues related to accountability, transparency, data privacy, intellectual property, and human rights [93], [94].

Biometric data are typically collected via biometric systems, which use a specific behavioral or physiological trait that is unique to all individuals [95]. Examples of biometric authentication include fingerprints, facial recognition, voice patterns and iris scanning [96], [97]. Biometric systems are a cornerstone of modern cybersecurity architecture and are preferred because they use characteristics linked to individual identities that are hard to replicate or forge, thus increasing security [54], [98].

As with previous technologies, AI's integration into biometric systems presents both opportunities and major challenges. AI provides greater accuracy, flexibility and intelligence to biometric authentication [99], [100]. AI uses machine learning and deep learning techniques to ensure that biometric systems learn to adapt swiftly to biological variances over time [101]. Biological variations can include biological changes due to health issues, environmental conditions, or even the passage of time [102], [103]. This more dynamic biological adaptability improves reliability and resilience. At the same time, serious questions are raised with AI, such as personal protection of data, questions of fairness and bias, misrepresentation and unauthorized surveillance.

From a legal perspective, biometric data constitute some of the most sensitive data available [104]. Unlike passwords or tokens, biometric identifiers cannot be altered or changed. If a person's biometric data are compromised, the risk associated with the use of biometric data is materially different. This very increased risk further elevates the legal burden on the companies that develop these systems in particular and therefore the responsibility to have legal protections designed for the provision of internal or external governance to limit the risks of these data. In fact, legal and regulatory frameworks such as the General Data Protection Regulation (GDPR) in the European Union classify biometric data as a "special category of personal data" and state that when biometric data are utilized, additional layers of protection must be in place when collecting, processing and storing biometric data [105]–[107]. Legal frameworks such as the emerging Artificial Intelligence Act, created by the European Union, aim to provide responses to the application of artificial intelligence, especially when it is used in biometric recognition or classification, when it recommends considerations of trustworthiness and transparency, and when it addresses risk [108].

On the other hand, the potential for artificial intelligence to improve biometric solutions is exciting, but new risks have emerged, as the security community has begun to recognize the potential for biometric systems to be vulnerable to adversarial attacks [109]–[111]. Adversarial examples, in the context of biometrics, are where biometric inputs (iris images, facial data, etc.) are modified in a way that is not detectable by humans but sufficiently changes the biometric encoder to mislead the recognition system [112]–[114]. The different types of adversarial attacks that are possible have profound implications for the immediate use of biometric authentication reliant on AI, as both unauthorized access and identity fraud are fundamental threats to the reliability and trustworthiness of biometric systems. It is important to identify and improve

systems to avoid or mitigate adversarial examples. Owing to the rate of technological adaptation and the evolution of civil liberty and criminality, legislation will need to establish new laws and expectations concerning the robustness and security of AI-enabled biometric technologies.

2.4. Recommendations for biometric security

Given the legal, ethical, and cybersecurity challenges associated with the use of biometric technologies, in countries where the system of laws is not strong enough to protect the public, it remains of paramount importance that serious actions are taken to ensure that biometric data are managed safely and responsibly. The first best practice recommendation is for Iraq to take quick action in enacting a comprehensive personal data protection law. The law should specifically identify biometric data as being particularly sensitive and protect them accordingly. The necessary data protection law must specify the criteria under which biometrics can be obtained and collected, utilized, stored, and shared in a manner compliant with international data protection standards such as the General Data Protection Regulation (GDPR) to protect individual rights. The legal framework must also mandate that written, explicit consent be obtained from individuals seeking to collect biometric data, especially employees. In so doing, individuals must be given sufficient transparency when obtaining consent, including reasonable information on why the data are being collected, the types of biometric data that may be collected, the length of time the data will be kept, and access to all the data. Possessing detailed information about an individual's rights increases their trust in the system being implemented and their trust and accountability more broadly in how to utilize it.

In addition, mandatory privacy impact assessments should be performed prior to the adoption of biometric technology, similar to other technologies adopted in communications and biometric systems in business when transitioning from assessments. Trust is not achieved by just making the assessments known, and organizations must be able to limit privacy risks and provide adequate technological and organizational measures to protect data privacy. Without that limitation of risk, it is not possible to establish trust in any new technology that is adopted.

Furthermore, critical measures need to include stronger standard encryption and authentication models and adapt them heedfully from the best practices seen right now with the biometric systems in different parts of the UAE and EU, or even where encryption and data security are legally mandated practices, organizations must augment the technical resilience of their biometric systems.

The establishment of an independent authority for data protection would include oversight and compliance, investigation of breaches, and possible sanctioning. The oversight will provide another layer of accountability to ensure that public trust of knowledgeable organization employers using biometric data is established not of the corporation but in their actions publicly and that there would be public accountability to protect personal rights.

Notably, there would need to be a concerted effort undertaken to train and educate judiciary and legal professionals on the protection of biometric data. Considering the importance of assisting individuals when their rights are being infringed upon creates a legal system capable of providing information on the intent of using biometric data while interpreting and enforcing laws that actually regulate the use of biometric data.

The intersection of artificial intelligence (AI), biometrics, and law necessitates the urgent need for interdisciplinary regulatory action. AI represents the technical excellence of biometric systems, whereas law ensures that the deployment of biometric systems exists in an ethical, transparent, human rights-amended environment. Legal duties must require AI-enhanced biometric systems to deploy effective impact assessment, accountability, and fairness measures to prevent discriminatory outcomes and interference with privacy rights.

In addition to technical feasibility, the future of secure biometric authentication will similarly rely on the robustness of the ethical and legal frameworks that accompany increased technological capabilities [115]. As technology evolves, law must evolve alongside many societal fronts, including consent, data minimization, purpose limitations, and the rights of individuals to challenge decisions made by automated systems [116]. Additionally, associations should increasingly collaborate to ensure that the advancement of AI can be effectively matched (and exceeded) by an equal advancement of legal and ethical frameworks [117], [118].

In summary, artificial intelligence has an immeasurable capacity to improve biometric authentication systems to be more accurate, flexible, and intelligent. However, this capability must be carefully balanced with legal obligations and ethics.

Given these opportunities and challenges, the current study aims to establish a new health-aware biometric authentication model that uses AI-based deep learning techniques to facilitate the critical issue of reliability, which is related to biometric variability. The study seeks to incorporate a legal and cybersecurity perspective in the development of the system. The methodology we propose aims to improve both the technical ability of iris-based authentication and the ability to pay attention to ethical obligations and laws. This approach allows the eventual product to be a credible system, which embodies data protection principles, mitigates risks, and builds user trust. The next chapter describes the detailed methodology used to achieve the goals of this research, which includes a description of dataset preparation, the deep learning architecture, and the evaluations used in the study.

3. METHODOLOGY

This chapter outlines the methodology used to design, develop and evaluate a health-aware biometric authentication system that is based on deep learning. The study looks to address and remediate the three primary issues identified in previous chapters, such as biometric variability, cybersecurity concerns and, finally, legal obligations, and another purpose of this study is to produce a reliable and legally aware model of iris-based biometric authentication. This chapter describes the selection of the dataset and its characteristics; the preprocessing tasks performed to improve the learning performance, architecture and training of the deep learning model (ResNet50); and the processes used to evaluate the classification accuracy and accuracy of the model, among other factors.

The methodology of this study consists of a structured four-stage sequence of (1) acquiring and preparing the dataset, (2) data preprocessing, (3) model development via deep learning techniques, and (4) model evaluation and performance analysis (see Figure 2).

Fig. 2. Methodology steps

3.1. Dataset Description

The dataset used in this study for iris health classification was a collection of samples from Kaggle [119], a trusted source for various datasets for machine learning. The iris health dataset includes 410 annotated images of human irises that fit into two health-related classes: mature and immature. The labels refer to the health status of the iris in relation to the status of cataracts, in which "mature" refers to a fully mature cataract present in the iris area, whereas "immature" refers to the early stages of the disease. In total, there are 214 unique "immature" labeled images and 196 unique "mature" labeled images. As shown in Figure 3, the sample images are of varying quality, resolution, brightness, eye color, and iris visibility, just as in any real-world scenario. This variability of features is necessary to allow deep learning models to learn how to distinguish between healthy irises and irises with respect to medical issues. This dataset was also selected because of its direct relevance to the objectives of the research, specifically, linking iris health assessments to the security component of biometric authentication.

Fig. 3. Classes of eyes

3.2. Data Preprocessing

The dataset was prepared for training the deep learning (DL) model via a purpose-built preprocessing pipeline. The first step was to pull the image paths and the class labels ("mature" or "immature") together into a pandas DataFrame, allowing easier manipulation and labeling throughout the workflow. The next step consisted of splitting the dataset into three sections via stratified sampling to maintain the class distribution, which resulted in a training set containing 70% of the images, a validation set containing 15% of the images, and a test set containing 15% of the images. This separation ensures that the DL model is exposed to patterns, whereas performance measures can be assessed on previously unseen data, essentially guaranteeing that the DL model is not biased. After the dataset was split into separate image sets, a label encoder (mapper) was employed to convert the categorical string labels to numerical labels, allowing the DL model to learn the target variable during supervised learning. In particular, the label "immature" was encoded as 0, and "mature" was encoded as 1. This stage of transformation facilitated the DL model's ability to learn the target variable correctly during training. Additional steps such as resizing, normalizing, and data augmentations (e.g., rotating the images, flipping the images) were applied to the images during the training of the DL model to increase generalizability and decrease the chance of overfitting.

3.3. Deep Learning Architecture

For the iris health classification task, a deep convolutional neural network with a ResNet50 architecture was used as the model because ResNet50 is a strong model that has been proven to perform well on image-labeling tasks. The ResNet50 model makes use of residual connections, which provide an elegant solution to the vanishing gradient problem that occurs when deeper networks are used [120]. Therefore, ResNet50 allows the use of just one model and utilizes the advantages of having a deeper network without markedly increasing training complexity [73], [121].

The ResNet50 model was initialized with weights that were pretrained on ImageNet, allowing the model to take advantage of previously learned low-level visual features such as edges, shapes, and textures [122], [123]. These weights serve as the basis for transfer learning, which enables the model to adjust or fine-tune the learning task of distinguishing “mature” iris conditions from “immature” iris conditions with less training time and improved accuracy. All the computations and training processes took place in a dedicated GPU environment, which allowed the training process to be completed more quickly and allowed for a decreased inference time (i.e., model taking an input and output label/classification). The model itself was implemented in PyTorch, and the model architecture was summarized (and hence double-checked) via the torchsummary package; this confirmed that the input shape and number of parameters were consistent. The model input consisted of images, which were resized to a resolution of 224 × 224 pixels and three color channels (RGBs). The model was trained with a standard batch size of 32, and each categorical label was converted to binary numerical format (where 0 was mapped to “immature” and where 1 was mapped to “mature”) via a manually constructed mapping function. The output dimension in the final classification layer was modified to one neuron for use with sigmoid activation, which is appropriate for this binary classification task.

The model was compiled and utilized binary cross-entropy loss and the standard Adam optimizer for progressively weighting the weight updates for the model. Conditional on evaluating training loss and validation accuracy, the training process stopped when validation loss began to persistently improve (to avoid overfitting and to ensure generalization).

3.4. Model evaluation

To evaluate the performance of the trained ResNet50 model, various key evaluation metrics, such as the confusion matrix, accuracy, precision, recall, and F1 score, were used [124], [125]. These metrics allow for understanding the model's ability to correctly classify iris health conditions as either “mature” or “immature”. Each metric provides an even greater level of detail when scrutinizing the model's classification performance.

The confusion matrix is a method of visualizing the classification model performance. It allows insight into how many true positives (TPs), true negatives (TNs), false positives (FPs), and false negatives (FNs) are generated [126]. These are essential for calculating the other metrics. A confusion matrix allows identification of not only how many classifications were accurate but also what types of errors were made. An "immature" iris is classified as "mature", or a "mature" iris is classified as "immature".

Accuracy is a widely used metric of classification [127]. It is the number of accurate predictions (both TP and TN) divided by the total number of predictions (TP + TN + FP + FN). It provides a good representation overall, but accuracy should always be considered with respect to learning from imbalanced data because it will not distinguish performance on separate classes.

Precision is the focus metric for the positive class and is calculated as the ratio of true positive predictions to the total number of positive predictions (TP + FP) [128]. It is how many of all "mature" iris classifications were true, and so a high precision means that when the model says "mature", it usually is.

Recall (sometimes referred to as the sensitivity or true positive rate) [129] is a metric that measures the ratio of true positive predictions to the total number of actual positives (TP + FN). It assesses how well the model identifies all actual "mature" irises. A high recall value would mean that the model successfully identified most of the actual "mature" irises correctly, even though perhaps some false positives could exist.

The F1 score reflects how we measure balanced performance as a single metric; both precision and recall can be combined into one score [130]. The F1 score is the harmonic mean of precision and recall and is especially useful when the data are imbalanced. F1 gives better weighting regardless of the lower value between precision and recall; thus, in the performance of the model, both aspects need to be evaluated.

In addition to these metrics, the fitting of the model was also established by looking at the learning curves (training and validation loss/accuracy) throughout training. The learning curves can shed light on whether the model is overfitting the data or underfitting the data. Overfitting to training data results in a continued decline in the training loss but an increase in the validation loss, which demonstrates that the validation performance plateaus at some point. To avoid time-consuming calculations through an arbitrary number of epochs as well as overfitting, I applied early stopping to halt training at the epoch of peak validation performance.

By observing the training accuracy and validation accuracy throughout the epochs, I was able to examine the exact learning process of the model. An ideal fitted model would yield high training and validation accuracy, which would also be similar to each other, indicating that the model was learning features despite not overfitting training examples. Throughout the analysis of the fitting curve, the model learned with the data without overfitting.

4. RESULT AND DISCUSSION

The performance of the ResNet50 model was assessed through various metrics, including accuracy, precision, recall, F1 score, and confusion matrix. The overall accuracy of the model was 98%, indicating that the model had a strong ability to differentiate between the two classes of "mature" and "immature" irides. The model shows a strong ability to generalize to new data and is able to provide accurate classifications.

The model's precision values were 0.97 for the "immature" class and 1.00 for the "mature" class. Precision indicates the proportion of true positive predictions out of the total number of positive predictions. The model's precision for the "mature" class is indicative that when the model predicts an iris as "mature", it is usually correct. The model's precision for the "immature" class is lower; however, it is still relatively high. A lower precision implies that some "immature" irides are misclassified as "mature" but have little effect on performance overall.

The model had a perfect recall score of 1.00 for the "immature" class, indicating that it accurately identified every occurrence of "immature" irises. The model for the "mature" class was slightly lower, with a recall score of 0.97, indicating that the model identified all but a few "mature" irises correctly. Additionally, the model's perfect recall regarding "immature" irides provides further evidence that the model accurately identifies early-stage cataracts, which is ultimately important in preventing false rejections from occurring in a biometric system.

The F1 score is composed of precision and recall in one metric (the harmonic mean), and it was 0.98 for the "immature" and "mature" classes. The model was able to consistently balance precision and recall, with the false positive and false negative totals being low as a result of balancing misclassifications. A high F1 score is particularly important when observing a healthcare or security scenario, as false rejections and acceptance carry substantial consequences.

The macro average precision, recall, and F1 score was 0.98, which means that the model had similar performance for the two classes without having an advantage for one class over the other class. The weighted average precision, recall, and F1 score were also 0.98, which accounts for the relative class distribution and indicates that the overall model performed well.

The confusion matrix was used to visualize the classification performance of the model in distinguishing between "mature" and "immature" irides. In the confusion matrix shown in Figure 4, the top-left cell indicates that 29 "immature" irides were accurately classified, and the bottom-right cell shows that 32 "mature" irides were accurately classified. There was also one misclassification where the model misclassified an "immature" iris as "mature". Overall, the overall total error was low, which ultimately indicates strong reliability. The separation of true positives and low false negative rates indicate that the model is reliable for classification in the biometric sense.

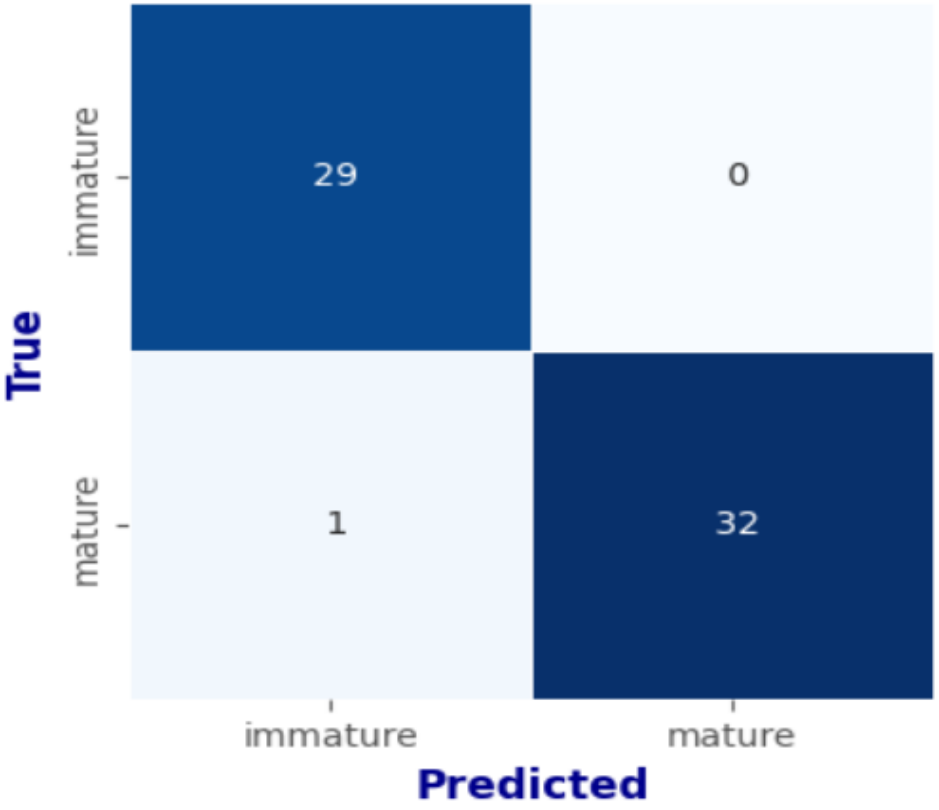

Fig. 4. Confusion matrix of the test

These significant results are especially notable in the context of the small data constraints mentioned above; however, the model clearly has good generalizability. The use of pretrained ResNet50 weights and transfer learning enabled this project to develop greater accuracy for each trained epoch, as the model could employ previously learned feature representations from very large image datasets (i.e., ImageNet) that sped the learning process and improved the model's accuracy.

The model fit in Figure 5 was evaluated via depth curve analysis of learning curves for cross-entropy loss and balanced accuracy for both the training set and the validation set across the 70 training epochs. The loss curve continuously decreased for both the training set and the validation set, indicating that the model learned consistently and accurately reduced its error during the training process. The fact that the balanced accuracies for both the training set and validation curves were very high and plateaued and thus almost entirely flat over epochs indicates effective generalization and learning for unseen data well without overfitting.

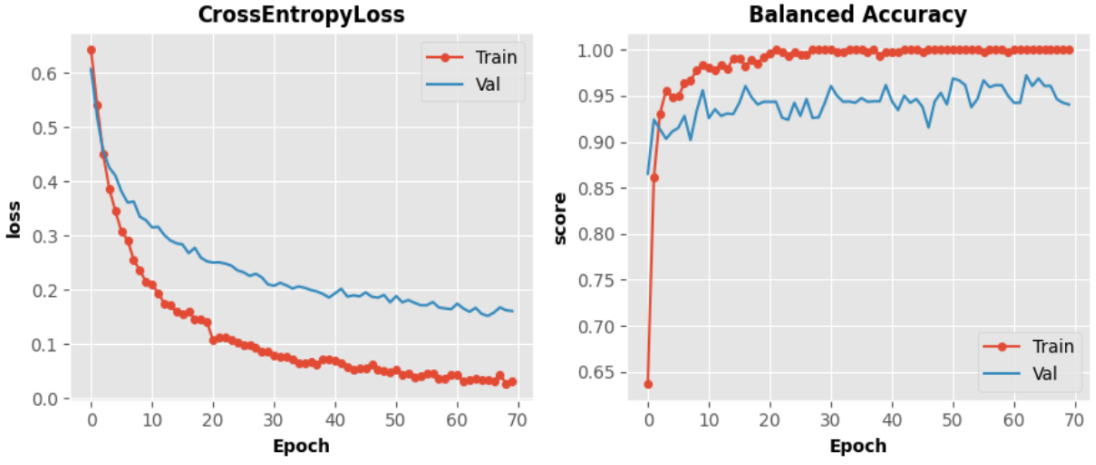

Fig. 5. Fitting of the dl model

This ability to achieve decreased loss and stable high accuracy demonstrates the model's strong ability to extract meaningful features from the data and its ability to be generalized to validation samples. The evaluation results highlight the suitability of the ResNet50 design for iris health classification. The model's accuracy, relative to the classification performance of state-of-the-art machine learning classifiers, can be a potential tool for iris-based biometric authentication systems. Giving resilient performance.

5. CONCLUSION AND FUTURE WORK

This study has successfully proven the potential interface between deep learning and biometric systems for developing cybersecurity measures. Using a ResNet50-based model for iris health classification, this study fills a major gap in biometric authentication systems by accounting for the variability in biometric traits attributable to human health conditions. The high performance of the model, with an accuracy rate of 98% and balanced precision and recall metrics, illustrates the effectiveness of the model, which can be classified as "mature" or "immature" and is related to the progression of cataracts.

Furthermore, the necessity of treating biometric data as a sensitive and immutable form of personal information, which requires an even greater cyber security protocol, is emphasized. A theoretical framework was formed that considered global legal standards such as the GDPR and highlighted biometric data protection in places such as Iraq, which has little to no protection. This absence of law put employees at risk but also put a 'crack in the foundation' of biometric authentication systems. The successful application of transfer learning and deep CNNs (ResNet50) for iris health classification supports the incorporation of AI-based health analysis with existing biometric frameworks and potentially reduces the impact of identity fraud and breaches that involve compromised biometric data.

This study is limited and recognizes that future work needs to address and further enhance the reach of the results. While the dataset in this study was diverse, it was not very large. Future research should also focus on the collection of larger datasets and more varied datasets to reflect an array of iris conditions, lighting environments, and demographic differences to increase the generalizability of the model. To deploy further in a live system (biometric system), models such as these would need to be further improved in terms of speed and efficiency to explore lightweight architectures suitable for edge devices.

Additionally, iris health analysis could also be integrated with a variety of other biometric models, such as facial recognition or fingerprint analysis, to build stronger security systems. Future research should also consider the ever-growing topic of adversarial attacks and explore the resilience of AI-based models that are deployed in biometric systems and develop the ability to detect and mitigate these types of attacks [131], [132]. Finally, using the insights gained from the legal perspective of this study, it is essential to investigate the framework for legal systems–both locally and intonationally–which can put in place extra individual rights protection in terms of ethical practices when using AI and biometric authentication systems.

In conclusion, the most innovative and secure, reliable and ethically sound systems integrate AI, biometric health analysis, and cybersecurity. The future of research in this area depends on future research and cross-disciplinary collaboration to avoid or at least address the growing challenges at the intersection of technology, law, and security.

Conflicts Of Interest

"The authors declare no conflicts of interest".

Funding

None.

Acknowledgment

None.

References

[1] S. A. Abdulrahman and B. Alhayani, “A comprehensive survey on the biometric systems based on physiological and behavioural characteristics,” *Mater. Today Proc.*, vol. 80, pp. 2642–2646, 2023, doi: 10.1016/j.matpr.2021.07.005.

[2] R. Alrawili, A. A. S. AlQahtani, and M. K. Khan, “Comprehensive survey: Biometric user authentication application, evaluation, and discussion,” *Comput. Electr. Eng.*, vol. 119, p. 109485, 2024, doi:

10.1016/j.compeleceng.2024.109485.

[3] Q. N. Tran, B. P. Turnbull, and J. Hu, "Biometrics and Privacy-Preservation: How Do They Evolve?," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 179–191, 2021, doi: 10.1109/ojcs.2021.3068385.

[4] S. Khade, S. Ahirrao, S. Phansalkar, K. Kotecha, S. Gite, and S. D. Thepade, "Iris liveness detection for biometric authentication: A systematic literature review and future directions," *Inventions*, vol. 6, no. 4, 2021, doi: 10.3390/inventions6040065.

[5] K. Nguyen, H. Proença, and F. Alonso-Fernandez, "Deep Learning for Iris Recognition: A Survey," *ACM Comput. Surv.*, vol. 56, no. 9, Apr. 2024, doi: 10.1145/3651306.

[6] T. Kumar, S. Bhushan, P. Sharma, and V. Garg, "Examining the Vulnerabilities of Biometric Systems," in *Leveraging Computer Vision to Biometric Applications*, Chapman and Hall/CRC, 2024, pp. 34–67. doi: 10.1201/9781032614663-3.

[7] M. Chaturvedi, M. Kaushik, S. Satija, and R. Kumar, "A STUDY ON ENHANCING DATA SECURITY AND CRIME DETECTION WITH COMPUTATIONAL INTELLIGENCE AND CYBERSECURITY".

[8] M. Amini and L. Javidnejad, "Legal Regulation of Biometric Data: A Comparative Analysis of Global Standards," *Leg. Stud. Digit. Age*, vol. 3, no. 1, pp. 26–34, 2024.

[9] P. Melzi, C. Rathgeb, R. Tolosana, R. Vera, and C. Busch, "An Overview of Privacy-Enhancing Technologies in Biometric Recognition," *ACM Comput. Surv.*, vol. 56, no. 12, Oct. 2024, doi: 10.1145/3664596.

[10] P. Voigt and A. Von dem Bussche, "The EU General Data Protection Regulation (GDPR)," *EU Gen. Data Prot. Regul.*, vol. 10, no. 3152676, pp. 10–5555, 2020, doi: 10.1093/oso/9780198826491.001.0001.

[11] C. J. Hoofnagle, B. van der Sloot, and F. Z. Borgesius, "The European Union general data protection regulation: What it is and what it means," *Inf. Commun. Technol. Law*, vol. 28, no. 1, pp. 65–98, 2019, doi: 10.1080/13600834.2019.1573501.

[12] N. Gruschka, V. Mavroeidis, K. Vishi, and M. Jensen, "Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR," in *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*, 2018, pp. 5027–5033. doi: 10.1109/BigData.2018.8622621.

[13] E. J. Kindt, "Privacy and Data Protection Issues of Biometric Applications A Comparative Legal Analysis," *Law, Gov. Technol. Ser.*, vol. 12, pp. 1–975, 2013.

[14] G. J. Voelz, *The Rise of IWAR: Identity, Information, and the Individualization of Modern Warfare*. Simon and Schuster, 2018. [Online]. Available: https://www.jstor.org/stable/resrep11804

[15] T. Bisztray, "Investigating Privacy Aspects of Identity Management: From Data Protection Impact Assessment for Biometric Applications to Privacy-Centric Password Testing," 2023, [Online]. Available: https://www.duo.uio.no/handle/10852/105551%0Ahttps://www.duo.uio.no/bitstream/handle/10852/105551/3/PhD-Bisztray-2023.pdf

[16] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electron.*, vol. 12, no. 6, 2023, doi: 10.3390/electronics12061333.

[17] M. Punia, A. Choudhary, S. Agarwal, and V. Shukla, "Ethical Considerations and Legal Frameworks for Biometric Surveillance Systems: The Intersection of AI, Soft Biometrics, and Human Surveillance," in *Lecture Notes in Networks and Systems*, A. Chaturvedi, S. U. Hasan, B. K. Roy, and B. Tsaban, Eds., Singapore: Springer Nature Singapore, 2024, pp. 659–674. doi: 10.1007/978-981-97-0641-9_45.

[18] E. S. Neal Joshua, N. T. Rao, and D. Bhattacharyya, "Managing information security risk and Internet of Things (IoT) impact on challenges of medicinal problems with complex settings," in *Multi-Chaos, Fractal and Multi-Fractional Artificial Intelligence of Different Complex Systems*, Y. Karaca, D. Baleanu, Y.-D. Zhang, O. Gervasi, and M. Moonis, Eds., Academic Press, 2022, pp. 291–310. doi: 10.1016/B978-0-323-90032-4.00007-9.

[19] J. R. Malgheet, N. B. Manshor, and L. S. Affendey, "Iris Recognition Development Techniques: A Comprehensive Review," *Complexity*, vol. 2021, no. 1, p. 6641247, 2021, doi: 10.1155/2021/6641247.

[20] B. Kaur and S. S. Saini, "Estimation towards the impact of contact lens in iris recognition: A study," *Multimed. Tools Appl.*, vol. 84, no. 8, pp. 4361–4392, 2024, doi: 10.1007/s11042-024-18818-4.

[21] Y. Yin, S. He, R. Zhang, H. Chang, and J. Zhang, "Deep learning for iris recognition: a review," *Neural Comput. Appl.*, 2025, doi: 10.1007/s00521-025-11109-5.

[22] M. Elhussein, A. Almuhaideb, F. Alholyal, R. Osman, and S. Elfaki, "Efficient Entry: A Stateful Authentication

Approach in Health-Aware Smart Gate Systems," *IEEE Access*, vol. 12, pp. 70634–70645, 2024, doi: 10.1109/ACCESS.2024.3398569.

[23] A. M. Almuhaideb *et al.*, "Design Recommendations for Gate Security Systems and Health Status: A Systematic Review," *IEEE Access*, vol. 11, pp. 131508–131520, 2023, doi: 10.1109/ACCESS.2023.3335115.

[24] A. Kintonova, I. Povkhan, M. Mussaif, and G. Gabdreshov, "Improvement of Iris Recognition Technology for Biometric Identification of a Person," *Eastern-European J. Enterp. Technol.*, vol. 6, no. 2–120, pp. 60–69, 2022, doi: 10.15587/1729-4061.2022.269948.

[25] A. Godfrey *et al.*, "Fit-for-Purpose Biometric Monitoring Technologies: Leveraging the Laboratory Biomarker Experience," *Clin. Transl. Sci.*, vol. 14, no. 1, pp. 62–74, 2021, doi: 10.1111/cts.12865.

[26] M. Gomez-Barrero *et al.*, "Biometrics in the Era of COVID-19: Challenges and Opportunities," *IEEE Trans. Technol. Soc.*, vol. 3, no. 4, pp. 307–322, 2022, doi: 10.1109/tts.2022.3203571.

[27] A. De Keyser, Y. Bart, X. Gu, S. Q. Liu, S. G. Robinson, and P. K. Kannan, "Opportunities and challenges of using biometrics for business: Developing a research agenda," *J. Bus. Res.*, vol. 136, pp. 52–62, 2021, doi: 10.1016/j.jbusres.2021.07.028.

[28] E. Awumey, S. Das, and J. Forlizzi, "A Systematic Review of Biometric Monitoring in the Workplace: Analyzing Socio-technical Harms in Development, Deployment and Use," in *2024 ACM Conference on Fairness, Accountability, and Transparency, FAccT 2024*, in FAccT '24. New York, NY, USA: Association for Computing Machinery, 2024, pp. 920–932. doi: 10.1145/3630106.3658945.

[29] K. Shaheed *et al.*, "A Systematic Review on Physiological-Based Biometric Recognition Systems: Current and Future Trends," *Arch. Comput. Methods Eng.*, vol. 28, no. 7, pp. 4917–4960, 2021, doi: 10.1007/s11831-021-09560-3.

[30] O. L. Finnegan *et al.*, "The utility of behavioral biometrics in user authentication and demographic characteristic detection: a scoping review," *Syst. Rev.*, vol. 13, no. 1, p. 61, 2024, doi: 10.1186/s13643-024-02451-1.

[31] Y. Zheng *et al.*, "Biometric identification of taxodium spp. And their hybrid progenies by electrochemical fingerprints," *Biosensors*, vol. 11, no. 10, 2021, doi: 10.3390/bios11100403.

[32] B. Meden *et al.*, "Privacy-Enhancing Face Biometrics: A Comprehensive Survey," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 4147–4183, 2021, doi: 10.1109/TIFS.2021.3096024.

[33] N. D. AL-Shakarchy, H. K. Obayes, and Z. N. Abdullah, "Person identification based on voice biometric using deep neural network," *Int. J. Inf. Technol.*, vol. 15, no. 2, pp. 789–795, 2023, doi: 10.1007/s41870-022-01142-1.

[34] A. Parashar, A. Parashar, A. F. Abate, R. S. Shekhawat, and I. Rida, "Real-time gait biometrics for surveillance applications: A review," *Image Vis. Comput.*, vol. 138, p. 104784, 2023, doi: 10.1016/j.imavis.2023.104784.

[35] I. Ebert, I. Wildhaber, and J. Adams-Prassl, "Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection," *Big Data Soc.*, vol. 8, no. 1, p. 20539517211013052, 2021, doi: 10.1177/20539517211013051.

[36] F. Jimmy, "Emerging Threats: The Latest Cybersecurity Risks and the Role of Artificial Intelligence in Enhancing Cybersecurity Defenses," *Int. J. Sci. Res. Manag.*, vol. 9, no. 02, pp. 564–574, 2021, doi: 10.18535/ijsrm/v9i2.ec01.

[37] R. Walters and M. Novak, *Cyber security, artificial intelligence, data protection & the law*. Springer, 2021.

[38] M. Hernandez-de-Menendez, R. Morales-Menendez, C. A. Escobar, and J. Arinez, "Biometric applications in education," *Int. J. Interact. Des. Manuf.*, vol. 15, no. 2–3, pp. 365–380, 2021, doi: 10.1007/s12008-021-00760-6.

[39] M. Hoffmann, M. Mariniello, and M. Hoffmann, "Biometric technologies at work : a proposed use-based taxonomy Executive summary," Bruegel, Brussels, 2021. [Online]. Available: https://hdl.handle.net/10419/270503

[40] V. Veeraiah, K. R. Kumar, P. Lalitha Kumari, S. Ahamad, R. Bansal, and A. Gupta, "Application of Biometric System to Enhance the Security in Virtual World," in *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2022*, 2022, pp. 719–723. doi: 10.1109/ICACITE53722.2022.9823850.

[41] B. Hassan, E. Izquierdo, and T. Piatrik, "Soft biometrics: a survey: Benchmark analysis, open challenges and recommendations," *Multimed. Tools Appl.*, vol. 83, no. 5, pp. 15151–15194, 2024, doi: 10.1007/s11042-021-10622-8.

[42] S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, "Biometrics recognition using deep learning: a survey," *Artif. Intell. Rev.*, vol. 56, no. 8, pp. 8647–8695, 2023, doi: 10.1007/s10462-022-10237-x.

[43] C. W. Lien and S. Vhaduri, "Challenges and Opportunities of Biometric User Authentication in the Age of IoT: A Survey," *ACM Comput. Surv.*, vol. 56, no. 1, Aug. 2023, doi: 10.1145/3603705.

[44] J. Laux, S. Wachter, and B. Mittelstadt, "Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk," *Regul. Gov.*, vol. 18, no. 1, pp. 3–32, 2024, doi: 10.1111/rego.12512.

[45] A. Ribera Martínez, "The Debiasing Paradox: Facial Recognition Technology and Biometric Identification Systems in the Artificial Intelligence Act," in *European Yearbook of Constitutional Law 2023: Constitutional Law in the Digital Era*, C. van Oirsouw, J. de Poorter, I. Leijten, G. van der Schyff, M. Stremler, and M. De Visser, Eds., The Hague: T.M.C. Asser Press, 2024, pp. 137–163. doi: 10.1007/978-94-6265-647-5_7.

[46] I. A. Bogoslov, S. Corman, and A. E. Lungu, "Perspectives on Artificial Intelligence Adoption for European Union Elderly in the Context of Digital Skills Development," *Sustain.* , vol. 16, no. 11, 2024, doi: 10.3390/su16114579.

[47] A. H. Lora, "CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK (CHAPTER III, SECTION 1)," *EU Regul. Artif. Intell. A Comment.*, p. 79, 2025.

[48] R. Montinaro, "Emotion Recognition and Personalized Adverting," *Eur. Rev. Priv. Law*, vol. 32, no. 6, pp. 1003–1036, 2024, doi: 10.54648/erpl2025012.

[49] P. Ruiu, S. Saiu, and E. Grosso, "Digital Identity in the EU: Promoting eIDAS Solutions Based on Biometrics," *Futur. Internet*, vol. 16, no. 7, 2024, doi: 10.3390/fi16070228.

[50] "BTIW '24: Proceedings of the Behavior Transformation by IoT International Workshop," New York, NY, USA: Association for Computing Machinery, 2024.

[51] J. Zhang, Z. Liu, and X. (Robert) Luo, "Unraveling juxtaposed effects of biometric characteristics on user security behaviors: A controversial information technology perspective," *Decis. Support Syst.*, vol. 183, p. 114267, 2024, doi: 10.1016/j.dss.2024.114267.

[52] A. Katirai, "Ethical considerations in emotion recognition technologies: a review of the literature," *AI Ethics*, vol. 4, no. 4, pp. 927–948, 2023, doi: 10.1007/s43681-023-00307-3.

[53] S. Ayeswarya and K. J. Singh, "A Comprehensive Review on Secure Biometric-Based Continuous Authentication and User Profiling," *IEEE Access*, vol. 12, pp. 82996–83021, 2024, doi: 10.1109/ACCESS.2024.3411783.

[54] S. Kumar, "Biometric Systems Security and Privacy Issues," in *Leveraging Computer Vision to Biometric Applications*, Chapman and Hall/CRC, 2024, pp. 68–91. doi: 10.1201/9781032614663-4.

[55] B. Menakadevi, D. S. Kumar, P. Nagasaratha, and K. Parimalam, "Biometric System Attacks-A Case Study," in *ICCECE 2025 - International Conference on Computer, Electrical and Communication Engineering*, 2025, pp. 1–7. doi: 10.1109/ICCECE61355.2025.10940734.

[56] H. K. Abdali, M. A. Hussain, Z. A. Abduljabbar, V. O. Nyangaresi, and A. J. Y. Aldarwish, "Comprehensive Challenges to E-government in Iraq," in *Lecture Notes in Networks and Systems*, R. Silhavy and P. Silhavy, Eds., Cham: Springer Nature Switzerland, 2024, pp. 639–657. doi: 10.1007/978-3-031-70300-3_47.

[57] M. Rahimi, "A Comprehensive Analysis of Privacy and Data Protection in Conflict-Affected Areas: Revising Human Rights and Humanitarian Law to Address the Challenges of Surveillance Technologies." 2024.

[58] L. Laishram, M. Shaheryar, J. T. Lee, and S. K. Jung, "Toward a Privacy-Preserving Face Recognition System: A Survey of Leakages and Solutions," *ACM Comput. Surv.*, vol. 57, no. 6, Feb. 2024, doi: 10.1145/3673224.

[59] M. Constantinides, E. Bogucka, S. Scepanovic, and D. Quercia, "Good Intentions, Risky Inventions: A Method for Assessing the Risks and Benefits of AI in Mobile and Wearable Uses," *Proc. ACM Hum.-Comput. Interact.*, vol. 8, no. MHCI, Sep. 2024, doi: 10.1145/3676507.

[60] M. A. Azer and R. Samir, "Overview of the Complex Landscape and Future Directions of Ethics in Light of Emerging Technologies," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 7, pp. 1459–1481, 2024, doi: 10.14569/IJACSA.2024.01507142.

[61] M. Mellon, "Facial Recognition Technology and the Dire Need to Regulate It," *SMU L. Rev. F.*, vol. 77, p. 272, 2024.

[62] C. Dul, "Facial Recognition Technology vs Privacy: The Case of Clearview AI," *Queen Mary Law J.*, vol. 3, p. 1, 2022, [Online]. Available: https://nissenbaum.tech.cornell.edu/papers/facial_recognition_report.pdf

[63] G. Gültekin Várkonyi, "Navigating data governance risks: Facial recognition in law enforcement under EU legislation," *INTERNET POLICY Rev. J. INTERNET Regul.*, vol. 13, no. 3, 2024.

[64] N. Khan and M. Efthymiou, "The use of biometric technology at airports: The case of customs and border protection (CBP)," *Int. J. Inf. Manag. Data Insights*, vol. 1, no. 2, p. 100049, 2021, doi: https://doi.org/10.1016/j.jjimei.2021.100049.

[65] M. Mäkelä, "Artificial intelligence to benefit the passenger experience at the airport," 2024.

[66] V. Wylde *et al.*, "Cybersecurity, Data Privacy and Blockchain: A Review," *SN Comput. Sci.*, vol. 3, no. 2, p. 127, 2022, doi: 10.1007/s42979-022-01020-4.

[67] H. M. S. S. Herath, H. M. K. K. M. B. Herath, B. G. D. A. Madhusanka, and L. G. P. K. Guruge, "Data Protection Challenges in the Processing of Sensitive Data," in *Data Protection: The Wake of AI and Machine Learning*, C. Hewage, L. Yasakethu, and D. N. K. Jayakody, Eds., Cham: Springer Nature Switzerland, 2024, pp. 155–179. doi: 10.1007/978-3-031-76473-8_8.

[68] C. Wu, "Data privacy: From transparency to fairness," *Technol. Soc.*, vol. 76, p. 102457, 2024, doi: https://doi.org/10.1016/j.techsoc.2024.102457.

[69] E. G. Popkova and K. Gulzat, "Technological Revolution in the 21st Century: Digital Society vs. Artificial Intelligence," in *The 21st Century from the Positions of Modern Science: Intellectual, Digital and Innovative Aspects*, E. G. Popkova and B. S. Sergi, Eds., Cham: Springer International Publishing, 2020, pp. 339–345.

[70] V.-D. Păvăloaia and S.-C. Necula, "Artificial Intelligence as a Disruptive Technology—A Systematic Literature Review," *Electronics*, vol. 12, no. 5, 2023, doi: 10.3390/electronics12051102.

[71] A. Albahri *et al.*, "Evaluating date fruit varieties for health benefits using advanced fuzzy decision-making," *Expert Syst. Appl.*, vol. 281, p. 127656, 2025, doi: https://doi.org/10.1016/j.eswa.2025.127656.

[72] M. A. Habeeb and Y. L. Khaleel, "Enhanced Android Malware Detection through Artificial Neural Networks Technique," *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 1 SE-Articles. pp. 62–77. doi: 10.58496/MJCS/2025/005.

[73] M. A. Habeeb, Y. L. Khaleel, R. D. Ismail, Z. T. Al-Qaysi, and A. F. N., "Deep Learning Approaches for Gender Classification from Facial Images," *Mesopotamian J. Big Data*, vol. 2024, pp. 185–198, 2024, doi: 10.58496/MJBD/2024/013.

[74] F. K. H. Mihna, M. A. Habeeb, Y. L. Khaleel, Y. H. Ali, and L. A. E. Al-Saeedi, "Using Information Technology for Comprehensive Analysis and Prediction in Forensic Evidence," *Mesopotamian J. CyberSecurity*, vol. 4, no. 1, 2024, doi: 10.58496/MJCS/2024/002.

[75] M. A. Habeeb, Y. L. Khaleel, and A. S. Albahri, "Toward Smart Bicycle Safety: Leveraging Machine Learning Models and Optimal Lighting Solutions," in *Proceedings of the Third International Conference on Innovations in Computing Research (ICR'24)*, K. Daimi and A. Al Sadoon, Eds., Cham: Springer Nature Switzerland, 2024, pp. 120–131.

[76] N. Kalra, P. Verma, and S. Verma, "Advancements in AI based healthcare techniques with FOCUS ON diagnostic techniques," *Comput. Biol. Med.*, vol. 179, p. 108917, 2024, doi: https://doi.org/10.1016/j.compbiomed.2024.108917.

[77] M. Bekbolatova, J. Mayer, C. W. Ong, and M. Toma, "Transformative Potential of AI in Healthcare: Definitions, Applications, and Navigating the Ethical Landscape and Public Perspectives," *Healthcare*, vol. 12, no. 2, 2024, doi: 10.3390/healthcare12020125.

[78] P. Weber, K. V. Carl, and O. Hinz, "Applications of Explainable Artificial Intelligence in Finance—a systematic review of Finance, Information Systems, and Computer Science literature," *Manag. Rev. Q.*, vol. 74, no. 2, pp. 867–907, 2024, doi: 10.1007/s11301-023-00320-0.

[79] S. Bahoo, M. Cucculelli, X. Goga, and J. Mondolo, "Artificial intelligence in Finance: a comprehensive review through bibliometric and content analysis," *SN Bus. Econ.*, vol. 4, no. 2, p. 23, 2024, doi: 10.1007/s43546-023-00618-x.

[80] K. Zhang and A. B. Aslan, "AI technologies for education: Recent research & future directions," *Comput. Educ. Artif. Intell.*, vol. 2, p. 100025, 2021, doi: 10.1016/j.caeai.2021.100025.

[81] X. Zhai *et al.*, "A Review of Artificial Intelligence (AI) in Education from 2010 to 2020," *Complexity*, vol. 2021, no. 1, p. 8812542, 2021, doi: 10.1155/2021/8812542.

[82] R. Espinel, G. Herrera-Franco, J. L. Rivadeneira García, and P. Escandón-Panchana, "Artificial Intelligence in Agricultural Mapping: A Review," *Agriculture*, vol. 14, no. 7, 2024, doi: 10.3390/agriculture14071071.

[83] A. A. Mana, A. Allouhi, A. Hamrani, S. Rehman, I. el Jamaoui, and K. Jayachandran, "Sustainable AI-based

production agriculture: Exploring AI applications and implications in agricultural practices," *Smart Agric. Technol.*, vol. 7, p. 100416, 2024, doi: https://doi.org/10.1016/j.atech.2024.100416.

[84] F. N. A. Fadya A Habeeb, Mustafa Abdulfattah Habeeb, Yahya Layth Khaleel, "Global Analysis and Prediction of CO2 and Greenhouse Gas Emissions across Continents," *Applied Data Science and Analysis*, vol. 2024 SE-. pp. 173–188. doi: 10.58496/ADSA/2024/014.

[85] A. Konya and P. Nematzadeh, "Recent applications of AI to environmental disciplines: A review," *Sci. Total Environ.*, vol. 906, p. 167705, 2024, doi: https://doi.org/10.1016/j.scitotenv.2023.167705.

[86] S. E. Dilsizian and E. L. Siegel, "Artificial Intelligence in Medicine and Cardiac Imaging: Harnessing Big Data and Advanced Computing to Provide Personalized Medical Diagnosis and Treatment," *Curr. Cardiol. Rep.*, vol. 16, no. 1, p. 441, 2013, doi: 10.1007/s11886-013-0441-8.

[87] M. Khalifa and M. Albadawy, "AI in diagnostic imaging: Revolutionising accuracy and efficiency," *Comput. Methods Programs Biomed. Updat.*, vol. 5, p. 100146, 2024, doi: https://doi.org/10.1016/j.cmpbup.2024.100146.

[88] I. H. Sarker, "AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems," *SN Comput. Sci.*, vol. 3, no. 2, p. 158, 2022, doi: 10.1007/s42979-022-01043-x.

[89] M. Javaid, A. Haleem, I. H. Khan, and R. Suman, "Understanding the potential applications of Artificial Intelligence in Agriculture Sector," *Adv. Agrochem*, vol. 2, no. 1, pp. 15–30, 2023, doi: https://doi.org/10.1016/j.aac.2022.10.001.

[90] W. Leal Filho *et al.*, "Deploying artificial intelligence for climate change adaptation," *Technol. Forecast. Soc. Change*, vol. 180, p. 121662, 2022, doi: https://doi.org/10.1016/j.techfore.2022.121662.

[91] S. O'Sullivan *et al.*, "Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery," *Int. J. Med. Robot. Comput. Assist. Surg.*, vol. 15, no. 1, p. e1968, 2019, doi: https://doi.org/10.1002/rcs.1968.

[92] Y. L. Khaleel, M. A. Habeeb, and T. O. C. EDOH, "Limitations of Deep Learning vs. Human Intelligence: Training Data, Interpretability, Bias, and Ethics," *Appl. Data Sci. Anal.*, vol. 2025, pp. 3–6, 2025, doi: 10.58496/ADSA/2025/002.

[93] F. K. H. M. H. A. S. L. A. E. A.-S. H. A. A.-T. M. A. H. Y. L. K. D. A. Mohammed, "Bridging Law and Machine Learning: A Cybersecure Model for Classifying Digital Real Estate Contracts in the Metaverse," *Mesopotamian J. Big Data*, vol. 2025, pp. 35–49, 2025, doi: 10.58496/MJBD/2025/003.

[94] A. S. Albahri, Y. L. Khaleel, and M. A. Habeeb, "The Considerations of Trustworthy AI Components in Generative AI; A Letter to Editor," *Appl. Data Sci. Anal.*, vol. 2023, pp. 108–109, 2023, doi: 10.58496/adsa/2023/009.

[95] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Syst. Appl.*, vol. 143, p. 113114, 2020, doi: https://doi.org/10.1016/j.eswa.2019.113114.

[96] U. B. Ghosh, R. Sharma, and A. Kesharwani, "Symptoms-Based Biometric Pattern Detection and Recognition," in *Augmented Intelligence in Healthcare: A Pragmatic and Integrated Analysis*, S. Mishra, H. K. Tripathy, P. Mallick, and K. Shaalan, Eds., Singapore: Springer Nature Singapore, 2022, pp. 371–399. doi: 10.1007/978-981-19-1076-0_19.

[97] Y. Moolla, A. De Kock, G. Mabuza-Hocquet, C. S. Ntshangase, N. Nelufule, and P. Khanyile, "Biometric Recognition of Infants using Fingerprint, Iris, and Ear Biometrics," *IEEE Access*, vol. 9, pp. 38269–38286, 2021, doi: 10.1109/ACCESS.2021.3062282.

[98] K. Krishna Prakasha and U. Sumalatha, "Privacy-Preserving Techniques in Biometric Systems: Approaches and Challenges," *IEEE Access*, vol. 13, pp. 32584–32616, 2025, doi: 10.1109/ACCESS.2025.3541649.

[99] A. I. Awad, A. Babu, E. Barka, and K. Shuaib, "AI-powered biometrics for Internet of Things security: A review and future vision," *J. Inf. Secur. Appl.*, vol. 82, p. 103748, 2024, doi: https://doi.org/10.1016/j.jisa.2024.103748.

[100] S. B. Abdullahi *et al.*, "Biometric Information Recognition Using Artificial Intelligence Algorithms: A Performance Comparison," *IEEE Access*, vol. 10, pp. 49167–49183, 2022, doi: 10.1109/ACCESS.2022.3171850.

[101] M. Ghilom and S. Latifi, "The Role of Machine Learning in Advanced Biometric Systems," *Electronics*, vol. 13, no. 13, 2024, doi: 10.3390/electronics13132667.

[102] E. Kruger, G. Porter, P. Birch, L. Bizo, and M. Kennedy, "The dimensions of 'forensic biosecurity' in genetic and facial contexts," *Secur. J.*, vol. 37, no. 4, pp. 1746–1768, 2024, doi: 10.1057/s41284-024-00445-1.

[103] S. G. L. Persiani, B. Kobas, S. C. Koth, and T. Auer, "Biometric Data as Real-Time Measure of Physiological Reactions to Environmental Stimuli in the Built Environment," *Energies*, vol. 14, no. 1, 2021, doi: 10.3390/en14010232.

[104] M. Smith and S. Miller, *Biometric identification, law and ethics*. Springer Nature, 2021.

[105] G. V. Cervi, "Why and How Does the EU Rule Global Digital Policy: an Empirical Analysis of EU Regulatory Influence in Data Protection Laws," *Digit. Soc.*, vol. 1, no. 2, p. 18, 2022, doi: 10.1007/s44206-022-00005-3.

[106] V. Stepenko, L. Dreval, S. Chernov, and V. Shestak, "EU Personal Data Protection Standards and Regulatory Framework," *J. Appl. Secur. Res.*, vol. 17, no. 2, pp. 190–207, 2022, doi: 10.1080/19361610.2020.1868928.

[107] C. Labadie and C. Legner, "Building data management capabilities to address data protection regulations: Learnings from EU-GDPR," *J. Inf. Technol.*, vol. 38, no. 1, pp. 16–44, 2023, doi: 10.1177/02683962221141456.

[108] N. T. Nikolinakos, *EU policy and legal framework for Artificial intelligence, Robotics and related Technologies-the AI Act*. Springer, 2023.

[109] Y. L. Khaleel, M. A. Habeeb, A. S. Albahri, T. Al-Quraishi, O. S. Albahri, and A. H. Alamoodi, "Network and cybersecurity applications of defense in adversarial attacks: A state-of-the-art using machine learning and deep learning methods," *J. Intell. Syst.*, vol. 33, no. 1, 2024, doi: 10.1515/jisys-2024-0153.

[110] H. M. Abdulfattah, K. Y. Layth, and A. A. Raheem, "Enhancing Security and Performance in Vehicular Adhoc Networks: A Machine Learning Approach to Combat Adversarial Attacks," *Mesopotamian J. Comput. Sci.*, vol. 2024, pp. 122–133, 2024, doi: 10.58496/MJCSC/2024/010.

[111] A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay, and D. Mukhopadhyay, "A survey on adversarial attacks and defences," *CAAI Trans. Intell. Technol.*, vol. 6, no. 1, pp. 25–45, 2021, doi: 10.1049/cit2.12028.

[112] A. Makrushin, A. Uhl, and J. Dittmann, "A Survey on Synthetic Biometrics: Fingerprint, Face, Iris and Vascular Patterns," *IEEE Access*, vol. 11, pp. 33887–33899, 2023, doi: 10.1109/ACCESS.2023.3250852.

[113] A. K. Jain, D. Deb, and J. J. Engelsma, "Biometrics: Trust, But Verify," *IEEE Trans. Biometrics, Behav. Identity Sci.*, vol. 4, no. 3, pp. 303–323, 2022, doi: 10.1109/TBIOM.2021.3115465.

[114] S. Marrone and C. Sansone, "On the transferability of adversarial perturbation attacks against fingerprint based authentication systems," *Pattern Recognit. Lett.*, vol. 152, pp. 253–259, 2021, doi: https://doi.org/10.1016/j.patrec.2021.10.015.

[115] M. Abdul-Al, G. Kumi Kyeremeh, R. Qahwaji, N. T. Ali, and R. A. Abd-Alhameed, "The Evolution of Biometric Authentication: A Deep Dive Into Multi-Modal Facial Recognition: A Review Case Study," *IEEE Access*, vol. 12, pp. 179010–179038, 2024, doi: 10.1109/ACCESS.2024.3486552.

[116] T. DoCarmo, S. Rea, E. Conaway, J. Emery, and N. Raval, "The law in computation: What machine learning, artificial intelligence, and big data mean for law and society scholarship," *Law \& Policy*, vol. 43, no. 2, pp. 170–199, 2021, doi: https://doi.org/10.1111/lapo.12164.

[117] A. Zafar, "Balancing the scale: navigating ethical and practical challenges of artificial intelligence (AI) integration in legal practices," *Discov. Artif. Intell.*, vol. 4, no. 1, p. 27, 2024, doi: 10.1007/s44163-024-00121-8.

[118] C. Cancela-Outeda, "The EU's AI act: A framework for collaborative governance," *Internet of Things*, vol. 27, p. 101291, 2024, doi: https://doi.org/10.1016/j.iot.2024.101291.

[119] "Cataract classification - wikidoc." https://www.wikidoc.org/index.php/Cataract_classification (accessed May 01, 2025).

[120] L. A. E. Al-saeedi *et al.*, "Artificial Intelligence and Cybersecurity in Face Sale Contracts: Legal Issues and Frameworks ," *Mesopotamian J. CyberSecurity*, vol. 4, no. 2 SE-Articles, pp. 129–142, Aug. 2024, doi: 10.58496/MJCS/2024/0012.

[121] Y. L. Khaleel, M. A. Habeeb, and M. A. Ahmed, "Refrigerator optimization: Leveraging RESnet method for enhanced storage efficiency," *AIP Conf. Proc.*, vol. 3264, no. 1, p. 40009, Mar. 2025, doi: 10.1063/5.0258460.

[122] B. Koonce, "ResNet 50," in *Convolutional Neural Networks with Swift for Tensorflow*, Berkeley, CA: Apress, 2021, pp. 63–72. doi: 10.1007/978-1-4842-6168-2_6.

[123] Y. L. Khaleel, M. A. Habeeb, and G. G. Shayea, "Integrating Image Data Fusion and ResNet Method for Accurate Fish Freshness Classification," *Iraqi J. Comput. Sci. Math.*, vol. 5, no. 4, p. 21, 2024.

[124] M. Heydarian, T. E. Doyle, and R. Samavi, "MLCM: Multi-Label Confusion Matrix," *IEEE Access*, vol. 10, pp. 19083–19095, 2022, doi: 10.1109/ACCESS.2022.3151048.

[125] G. Naidu, T. Zuva, and E. M. Sibanda, "A Review of Evaluation Metrics in Machine Learning Algorithms," in *Artificial Intelligence Application in Networks and Systems*, R. Silhavy and P. Silhavy, Eds., Cham: Springer International Publishing, 2023, pp. 15–25.

[126] R. Susmaga, "Confusion Matrix Visualization," in *Intelligent Information Processing and Web Mining*, M. A. Kłopotek, S. T. Wierzchoń, and K. Trojanowski, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 107–116.

[127] M. Muntean and F.-D. Militaru, "Metrics for Evaluating Classification Algorithms," in *Education, Research and Business Technologies*, C. Ciurea, P. Pocatilu, and F. G. Filip, Eds., Singapore: Springer Nature Singapore, 2023, pp. 307–317.

[128] M. Grandini, E. Bagli, and G. Visani, "Metrics for multi-class classification: an overview," *arXiv Prepr. arXiv2008.05756*, 2020.

[129] H. R. Sofaer, J. A. Hoeting, and C. S. Jarnevich, "The area under the precision-recall curve as a performance metric for rare binary events," *Methods Ecol. Evol.*, vol. 10, no. 4, pp. 565–577, 2019, doi: https://doi.org/10.1111/2041-210X.13140.

[130] D. Chicco and G. Jurman, "The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation," *BMC Genomics*, vol. 21, no. 1, p. 6, 2020, doi: 10.1186/s12864-019-6413-7.

[131] G. G. Shayea, M. H. M. Zabil, M. A. Habeeb, Y. L. Khaleel, and A. S. Albahri, "Strategies for protection against adversarial attacks in AI models: An in-depth review," *J. Intell. Syst.*, vol. 34, no. 1, p. 20240277, 2025, doi: 10.1515/jisys-2024-0277.

[132] Y. L. Khaleel, H. M. Abdulfattah, and H. Alnabulsi, "Adversarial Attacks in Machine Learning: Key Insights and Defense Approaches," *Appl. Data Sci. Anal.*, vol. 2024, pp. 121–147, 2024, doi: 10.58496/ADSA/2024/011.

[133] S. F. M. Al-Najjar, "Criminal responsibilities arising from artificial intelligence crimes," *Imam Ja'afar Al-Sadiq University Journal of Legal Studies*, vol. 4, no. 1, Art. 5, 2024. [Online]. Available: https://ijsu.researchcommons.org/ijsu/vol4/iss1/5

[134] F. Yohanna and S. I. Suleiman, "The impact of artificial intelligence on creativity, innovation and intellectual property rights in Nigeria," *Imam Ja'afar Al-Sadiq University Journal of Legal Studies*, vol. 4, no. 2, Art. 6, 2024. [Online]. Available: https://ijsu.researchcommons.org/ijsu/vol4/iss2/6