electronics

MDPI

Article

Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence

William Villegas-Ch * and Joselin García-Ortiz

Escuela de Ingeniería en Ciberseguridad, Facultad de Ingenierías Ciencias Aplicadas, Universidad de Las Américas, Quito 170125, Ecuador; joselin.garcia.ortiz@udla.edu.ec

* Correspondence: william.villegas@udla.edu.ec; Tel.: +593-98-136-4068

Abstract: The rapid expansion of artificial intelligence poses significant challenges in terms of data security and privacy. This article proposes a comprehensive approach to develop a framework to address these issues. First, previous research on security and privacy in artificial intelligence is reviewed, highlighting the advances and existing limitations. Likewise, open research areas and gaps that require attention to improve current frameworks are identified. Regarding the development of the framework, data protection in artificial intelligence is addressed, explaining the importance of safeguarding the data used in artificial intelligence models and describing policies and practices to guarantee their security, as well as approaches to preserve the integrity of said data. In addition, the security of artificial intelligence is examined, analyzing the vulnerabilities and risks present in artificial intelligence systems and presenting examples of potential attacks and malicious manipulations, together with security frameworks to mitigate these risks. Similarly, the ethical and regulatory framework relevant to security and privacy in artificial intelligence is considered, offering an overview of existing regulations and guidelines.

Keywords: AI privacy; AI security; data protection

check for updates

Citation: Villegas-Ch, W.; García-Ortiz, J. Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence. *Electronics* **2023**, *12*, 3786. https://doi.org/10.3390/electronics12183786

Academic Editor: Aravind Prakash

Received: 26 July 2023
Revised: 31 August 2023
Accepted: 5 September 2023
Published: 7 September 2023

1. Introduction

Artificial intelligence (AI) has experienced remarkable growth in recent years, and its application extends to various spheres of society, such as commerce, healthcare, transportation, and security. As AI becomes increasingly ubiquitous, addressing security and privacy concerns is essential. The increasing use of personal data in AI models poses significant challenges in protecting sensitive information. In this context, it becomes imperative to develop a robust and practical framework to ensure the security and confidentiality of AI [1].

Therefore, data protection in the context of AI has become a central concern. The data used to train the AI models may contain personal and sensitive information, such as names, addresses, and medical histories [2]. It is essential to understand the importance of protecting these data since their exposure or misuse can severely impact privacy and individual rights [3]. In this section, the importance of safeguarding data used in AI will be explored, policies and practices for its protection will be described, and examples of approaches used to preserve data integrity will be presented.

When developing a practical framework, AI security becomes another critical aspect that must be addressed. AI systems may face various vulnerabilities and be susceptible to attacks, such as the manipulation of input data or the exploitation of vulnerabilities in algorithms. These attacks can have significant consequences, such as the manipulation of results or the compromised privacy and security of users [4]. In the age of AI, privacy has become a fundamental right that must be protected. Collecting and processing large amounts of personal data pose significant challenges to individual privacy. Therefore, it is crucial to address the privacy challenges associated with AI and take steps to protect personal information. In addition to data protection, security, and privacy, it is also essential to consider the regulatory and ethical framework surrounding AI. Regulatory and ethical frameworks establish guidelines to ensure the responsible and ethical use of AI, especially in terms of security and privacy [5].

This research aims to develop a comprehensive framework to ensure security and privacy in AI. To achieve this purpose, a comprehensive review of related works is carried out to analyze the progress of AI security and confidentiality. In addition, a practical approach is proposed that covers crucial aspects such as data protection in AI, the security of AI systems, individual privacy, and relevant regulatory and ethical frameworks. A case study is carried out to evaluate the efficiency achieved, which allows for the quantitative measurement of the results obtained in critical areas, such as facial recognition, privacy, data retention, access and authorizations, and data quality. In addition, metrics such as facial recognition accuracy, facial recognition recall, balanced accuracy, data protection assessment, and data retention assessment are included.

Through the evaluation of data and analysis, concrete results are presented that allow for comparing and highlighting the strengths and contributions of the proposed framework in quantitative and qualitative terms. Finally, the results obtained with existing related works are discussed and compared, highlighting the strengths and contributions of the proposed framework. Ultimately, the importance of developing and adopting robust frameworks in AI is highlighted, along with the additional perspectives and challenges that require attention in this ever-evolving area.

This work is divided into the following sections considered vital to achieve the proposed objectives. Section 2 describes the materials and method; Section 3 presents the results obtained from the analysis; Section 4 presents the discussion of the results obtained with the proposal to improve security in systems with AI; and Section 5 presents the conclusions found in the development of the work.

2. Materials and Methods

In developing this approach, several key concepts are used to address security and privacy in the context of AI. First, a framework is established that provides a structure to ensure the protection of AI systems against threats and attacks and to preserve the confidentiality of data and personal information. AI security involves implementing security measures, audits, and controls that prevent unauthorized access and malicious manipulation of systems. On the other hand, privacy in AI focuses on safeguarding personal data, including obtaining proper consent and preventing unauthorized disclosures [6,7]. To achieve data protection, encryption techniques, anonymization, and minimization of the collection of personal information are used. In addition, existing regulatory and ethical frameworks that establish guidelines on the responsible use of AI and the protection of privacy are considered. These concepts are integrated to develop a comprehensive approach to ensuring security, privacy, and ethical compliance in implementing AI.

2.1. Review of Related Works

Reviewing related works, an analysis and comparison of several leading AI security and privacy positions have been conducted. In this process, an attempt has been made to identify each of their common and distinctive characteristics. This allows for an understanding of how security and privacy challenges are addressed in different contexts and how it contributes to existing research.

The work [8] highlights the importance of privacy in machine learning and highlights privacy-preserving solutions used to protect sensitive data. Similarly, in [9], membership inference attacks are discussed, which are relevant in our context since they can compromise data privacy. In [10], differential privacy is introduced, which we share as a critical aspect of our approach. In addition, Ref. [11] highlights secure multi-party computing (MPC) as a form of secure collaboration in data processing, which is also reflected in our methodology.

The review of related works highlights various approaches and solutions employed in AI security and privacy. These papers offer a solid foundation for understanding the challenges and strategies to ensure safety and confidentiality in developing and deploying AI systems [12]. By carrying out a comparative analysis of the works reviewed, it is possible to identify the strengths and limitations of each one [13]. Some common strengths include proposing innovative solutions, focusing on specific security and privacy issues, and presenting solid experimental results. However, there are limitations, such as the applicability in particular contexts, the scalability and performance of the proposed solutions, and the lack of consideration of specific scenarios or threats [14].

In this Table 1, four relevant investigations are presented that address fundamental aspects of security and privacy in the context of AI. Each study has been carefully selected to highlight its primary focus, the technologies used, and the results obtained.

Table 1. Comparison of relevant research on AI security and privacy.

Investigation	Focus	Used Technology	Featured Results
[15]	Data anonymization	Encryption techniques	Reduction in the risk of identification of sensitive data in facial recognition systems.
[16]	Reliability assessment in AI systems	Machine learning models	Significant reliability improvement.
[17]	Differential privacy in AI models	Differential privacy protocols	Adequate protection of individual privacy during training of AI models.
[5]	AI privacy and security framework	Homomorphic encryption	Successful implementation of a complete framework to guarantee security and privacy in AI systems.

The comparison table provides an overview of the most prominent approaches and achievements in AI security and privacy, highlighting the diversity of technologies used and the results achieved in each investigation. These findings contribute significantly to AI security and privacy progress and provide a solid foundation for future research and technological advances.

Despite the advances made in AI security and privacy, there are still gaps and open areas of research that require attention. For example, as the adoption of pre-trained models increases, it is essential to address the sensitivity of the data used in training and how to protect sensitive information during use. Furthermore, with the growth of real-time AI applications, it is critical to research and develop efficient and effective privacy approaches in real-time data processing without compromising the security or privacy of sensitive data.

Our work differentiates itself by approaching these approaches and solutions more holistically. We consider individual security and privacy aspects and integrate different solutions into a coherent framework. Furthermore, through our case study methodology, we have applied these solutions in a practical context, demonstrating their effectiveness and complementarity in an actual facial recognition application.

2.2. Data Protection in AI

The security and privacy of the data used to train AI models are paramount. Protecting these data is crucial because they may contain sensitive and private information of individuals or entities. If these data were to fall into the wrong hands or are misused, there may be privacy violations and negative consequences [18]. Additionally, the quality and representativeness of training data are critical to ensuring that AI models are accurate, fair, and reliable. Therefore, data protection is essential to building trust in AI systems.

To safeguard sensitive data used in AI, it is necessary to implement appropriate policies and practices. This involves establishing access controls to limit who can access and use the data and implementing security measures to prevent unauthorized access. It is also essential to have data anonymization or pseudonymization procedures, whereby identities or personally identifiable information are removed or masked to protect individuals' privacy [19]. In addition, encryption techniques may be used to ensure the confidentiality of data during storage and transmission.

There are various approaches to preserve the integrity of the data used in AI. One involves data validation and cleaning techniques to ensure quality and eliminate possible biases or errors [20]. In addition, anomaly detection techniques and pattern analysis can be applied to identify possible manipulations or malicious attacks on the training data. In addition, federated learning techniques can be used, in which data are kept in their original locations and only updated models are shared, thus minimizing the exposure of sensitive data.

2.3. AI Security

The security of AI systems has become a growing concern due to the vulnerabilities and risks associated with their implementation. These systems can be exposed to various vulnerabilities and security risks. These vulnerabilities can arise due to the lack of robustness in the AI algorithms, the manipulation of the training data, the initial design of the systems, or the exploitation of weaknesses in the implementations. These risks can manifest in adversarial attacks, model manipulation, unwanted biases, confidential information leaks, or unfair and detrimental decision-making [21]. Different types of attacks and malicious manipulations can compromise the security of AI systems. Some examples include:

- Adversarial attacks: An adversary may trick or manipulate an AI model by introducing malicious data or crafting specific inputs to evade detection and obtain undesirable results. These attacks can have severe consequences in critical applications, such as manipulating security systems, fraud, or phishing attacks.
- Manipulation of training data: The data used to train AI models can be manipulated to introduce biases, distorted representations, or malicious information. This can affect the accuracy and reliability of the models and potentially lead to erroneous or discriminatory decisions [22].
- Exploitation of vulnerabilities in AI systems: AI systems may be vulnerable to cyberattacks, such as malicious code injection, information theft, or denial of service. These attacks can compromise the integrity of the models and the confidentiality of the data used in the AI process.

To mitigate security risks in AI systems, it is crucial to implement proper security frameworks. These frameworks comprise security practices and measures, including:

- Security assessment and testing: Security and penetration tests should be performed on AI systems to identify potential vulnerabilities and weaknesses. This involves analyzing AI models, data used, and technical implementations for potential risks.
- Implementation of access controls: It is necessary to establish appropriate access controls to ensure that only authorized persons can access AI systems and sensitive data.
- Continuous monitoring: It is essential to constantly monitor AI systems to detect suspicious activity, attacks, or malicious manipulation. Monitoring can include anomaly detection, tracking model output, and tracking unauthorized access attempts [23].
- Updates and patches: AI systems must be updated with the latest security updates and patches to mitigate known vulnerabilities and ensure protection against new attacks.

By following these security frameworks, risks can be reduced, and the security of AI systems can be strengthened. However, it is essential to note that AI security is an ongoing challenge as adversaries and threats are constantly evolving. Therefore, staying current on AI's latest research and security practices is necessary.

2.4. AI Privacy

Privacy is critical in AI, as using large amounts of personal data can pose significant challenges. For example, AI uses large volumes of personal data to train models and make inferences. This may include sensitive data, such as medical information, personal preferences, or location data. As a result, there is a need to address privacy challenges to ensure personal data are handled securely and ethically [24]. Managing personal data in AI involves adopting policies and practices to protect individual privacy. This consists of obtaining individuals' informed consent to collect and use their data and ensuring that privacy principles are adhered to, such as minimizing information collection and limiting the use of data to only pre-agreed purposes [25,26].

To protect privacy in AI, various techniques and approaches are used. Some of them include:

- Data anonymization: Data anonymization techniques may be applied to remove or mask personally identifiable information from datasets used in AI. This ensures that data cannot be directly associated with specific individuals, thus preserving privacy.
- Minimizing the collection of personal information: The practice of reducing the collection of unnecessary personal information in AI systems may be adopted [27]. This involves limiting the amount of personal data collected and using techniques such as aggregation and tokenization to reduce the exposure of personally identifiable information.
- Use of differential privacy techniques: Differential privacy is a technique that adds controlled noise to the data so that the AI results do not reveal sensitive information about specific individuals. This protects an individual's data privacy without compromising the model's utility [28].
- In the process of developing AI systems, it is essential to adopt an approach that emphasizes privacy. This means considering privacy issues in all phases of the AI lifecycle, from data collection to model deployment, to address privacy challenges adequately.

The implementation of these techniques and approaches allows us to find a balance between the use of personal data to drive AI and the protection of individual privacy. However, it is of the utmost importance to bear in mind that confidentiality in AI must be addressed comprehensively and in line with current legal and regulatory frameworks, such as the General Data Protection Regulation (GDPR) in the European Union.

2.5. Proposed Framework to Ensure the Security and Privacy of AI

In the framework, the unique features of each aspect have been identified: "Security" focuses on protecting the AI system and data against threats and attacks. In contrast, "Privacy" focuses on protecting personal and sensitive data and guarantee ethical and responsible use.

2.5.1. Special Features

The unique feature of security in AI focuses on protecting the AI system and its data against potential threats and attacks. This involves implementing measures to prevent and mitigate security risks, such as unauthorized access to data, input tampering, or exploiting vulnerabilities in the algorithm. Security also ensures AI systems' integrity, confidentiality, and availability.

The unique feature of privacy in AI refers to protecting personal and sensitive data used in AI systems. This involves ensuring that data are used ethically and responsibly, respecting individual rights, and preventing unauthorized disclosure or misuse of personal information. Privacy is also concerned with ensuring that data are kept confidential and used only for previously agreed purposes.

2.5.2. Consideration in the Comprehensive Framework

In the comprehensive framework, different components and approaches were designed to address both security and privacy effectively and coherently:

- Data Protection Policies and Practices: We establish robust policies and practices to ensure that the data used in the AI system are adequately protected, preventing unauthorized access and tampering.
- Data Anonymization Techniques: We apply data anonymization techniques to protect the identity of individuals and ensure that data are used in an aggregated or de-identified manner where possible.
- Data Encryption: We implement data encryption to protect the confidentiality and integrity of data in transit and at rest, thus preventing unauthorized third parties from accessing sensitive information.
- Access Monitoring and Audits: We establish monitoring and auditing mechanisms to supervise access to the AI system and detect possible security violations or unauthorized access attempts.
- Privacy Assessment: We conduct a privacy assessment to ensure that personal data are used ethically and responsibly, in compliance with applicable privacy regulations and standards.
- Security Assessment: We perform a security assessment to identify and mitigate potential vulnerabilities and security risks in the AI system.

These approaches and measures ensure that security and privacy are fully considered in the framework, keeping clear boundaries between both features and ensuring robust and reliable protection in AI.

2.6. Regulatory and Ethical Framework

AI security and privacy are subject to ethical and legal frameworks that seek to ensure the responsible and ethical use of this technology. Recently, there has been a growing interest in AI regulation to address the associated risks and challenges. Various countries and organizations have developed regulatory and ethical frameworks to promote security and privacy in AI. At the international level, multiple organizations and entities have issued guidelines and ethical principles for creating and using AI [29]. For example, the Organization for Economic Cooperation and Development (OECD) has established AI regulations emphasizing transparency, responsibility, and inclusiveness. Likewise, the European Commission has published ethical guidelines for trustworthy AI based on fairness, privacy, and transparency.

At the regional level, the European Union's General Data Protection Regulation (GDPR) establishes a legal framework for protecting personal data, including those used in AI. This regulation defines the rights of individuals regarding the processing of their data and establishes obligations for the organizations that handle said data. At the national level, several countries have enacted specific laws and regulations to address AI security and privacy [30]. For example, the Brazilian Personal Data Protection Law (LGPD) establishes principles and standards for processing personal data, including their use in AI systems. Similarly, the California Consumer Data Protection Act (CCPA) in the United States addresses personal data privacy, including AI-related data.

It is crucial to remember that regulatory and ethical frameworks are constantly evolving as a better understanding of AI-related challenges and risks is gained. Therefore, it is essential to keep up to date with the updates and changes in the corresponding regulations and to comply with the ethical principles and best practices established in each jurisdiction.

2.6.1. Framework for AI Security and Privacy

The creation of this framework provides a structured guide to ensure security and privacy in the field of AI. This framework builds on the aspects discussed previously and will serve as a reference for organizations wishing to implement strong security and privacy measures in their AI systems [31]. Developing this framework involves considering several key elements:

- Risk assessment: A thorough assessment of the risks associated with AI systems must be conducted. This involves identifying potential threats and vulnerabilities and assessing their impact on AI security and privacy.
- Data protection policies and practices: Establishing firm policies and practices to protect the data used in AI systems is essential. This includes implementing access controls, encrypting sensitive data, properly managing consent, and adopting principles such as minimizing data collection and retaining data only for as long as necessary.
- AI model security measures: Security measures must be implemented to protect AI models. This implies guaranteeing the model's integrity, protecting it against attacks by adversaries, and ensuring its confidentiality [32].
- Monitoring and threat detection: It is necessary to establish monitoring and detection mechanisms to identify potential threats and attacks on AI systems. This may include implementing intrusion detection systems, log analysis, and the real-time monitoring of AI operations.
- Transparency and explainability mechanisms: Mechanisms must be established to guarantee the transparency and explainability of AI systems. This involves appropriately documenting the AI model training process and decision-making processes and providing clear and understandable information about how data are used and how results are generated.
- Evaluation and continuous improvement: The framework should focus on evaluation and constant improvement. This involves conducting regular security and privacy audits, penetration testing, reviewing, and updating policies and practices, and staying current on the latest AI security and privacy research and development.

By implementing and adopting this framework, organizations can establish a solid foundation for ensuring the security and privacy of AI in their operations [33]. However, it is essential to note that each organization will have specific considerations and requirements. Therefore, it is necessary to adapt and customize this framework according to the individual needs of each entity.

2.6.2. Development of a Framework to Guarantee the Security and Privacy of AI

Developing a framework to ensure the security and privacy of AI becomes a critical element of an environment increasingly driven by AI. Implementing AI systems carries potential data protection, safety, and privacy risks, highlighting the need to establish robust and practical measures. In this sense, creating an adequate framework provides a structured guide to address these challenges, ensuring the protection of data and AI models and in compliance with ethical and legal principles.

Figure 1 presents the critical stages for the development of the framework. It starts with the scoping of the framework, where the objectives and specific scope are stated, i.e., what security and privacy aspects of AI will be addressed and what the framework is intended to achieve. A comprehensive assessment of risks and threats that could affect the security and privacy of AI systems is then carried out. At this stage, chances are identified and classified based on their severity and probability of occurrence. Risk mitigation strategies are developed if risks are identified, and the process concludes with an implementation of those strategies [34]. If it is not possible to identify and classify the risks, we proceed to implement data protection policies and practices. At this stage, policies and procedures are established to safeguard the data used in the AI systems, such as access controls, data encryption, and proper consent management.

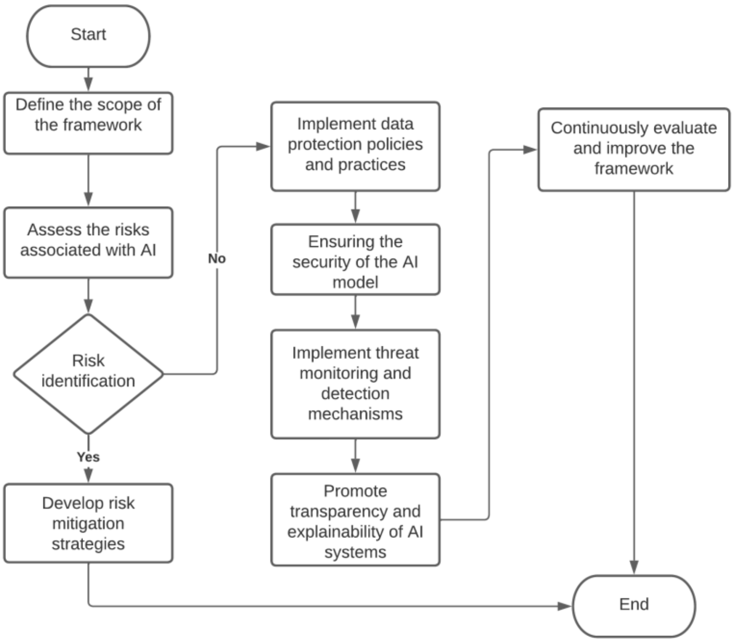
Start
Define the scope of the framework
Assess the risks associated with AI
Risk identification
No
Yes
Develop risk mitigation strategies
Implement data protection policies and practices
Ensuring the security of the AI model
Implement threat monitoring and detection mechanisms
Promote transparency and explainability of AI systems
Continuously evaluate and improve the framework
End

Figure 1. Flowchart for the development of a framework that guarantees the security and privacy of AI.

In the next stage, privacy principles are applied, such as minimizing data collection and retaining data for as long as necessary. These principles guarantee the security of the AI model, where security measures are implemented to protect the AI models, such as defense techniques against adversary attacks, and ensure the integrity and confidentiality of the model [35]. Subsequently, threat detection mechanisms and monitoring systems are implemented to identify possible threats and attacks on AI systems. Log analysis and intrusion detection tools and techniques can detect abnormal behavior.

Next, the transparency and explainability of AI systems are promoted, which implies adequately documenting AI models' training and decision-making processes. Clear and understandable information is provided on the use of data and the generation of AI results. Finally, an evaluation and continuous improvement of the framework are carried out. This involves conducting regular security and privacy audits to assess the framework's effectiveness. Also, penetration tests and vulnerability scans are conducted to identify possible security gaps [36,37]. It is essential to stay updated with the latest research and advancements in AI security and privacy and make any necessary updates to the framework accordingly.

3. Results

Data protection has been considered in an AI-based facial recognition system to evaluate the framework. This application has been developed in a small organization that uses a facial recognition AI system to access critical areas, such as data centers, to improve security and access control. However, the organization recognizes the importance of protecting personal data used by the system and has implemented the AI security and privacy framework to address these challenges.

Figure 2 presents the stages to implement the framework, considering the data protection policies and practices developed in the previous sections. In the first stage, the main objective is established, which is to evaluate the effectiveness of the AI security and privacy framework in protecting personal data used in the facial recognition system. In the next stage, data collection and preparation are carried out, which consists of collecting facial features and personal attributes to evaluate the performance of the facial recognition system. Finally, the AI security and privacy framework is implemented in the next stage. This involves defining data protection policies and practices, applying data anonymization techniques, implementing data encryption, and establishing access monitoring and auditing mechanisms.

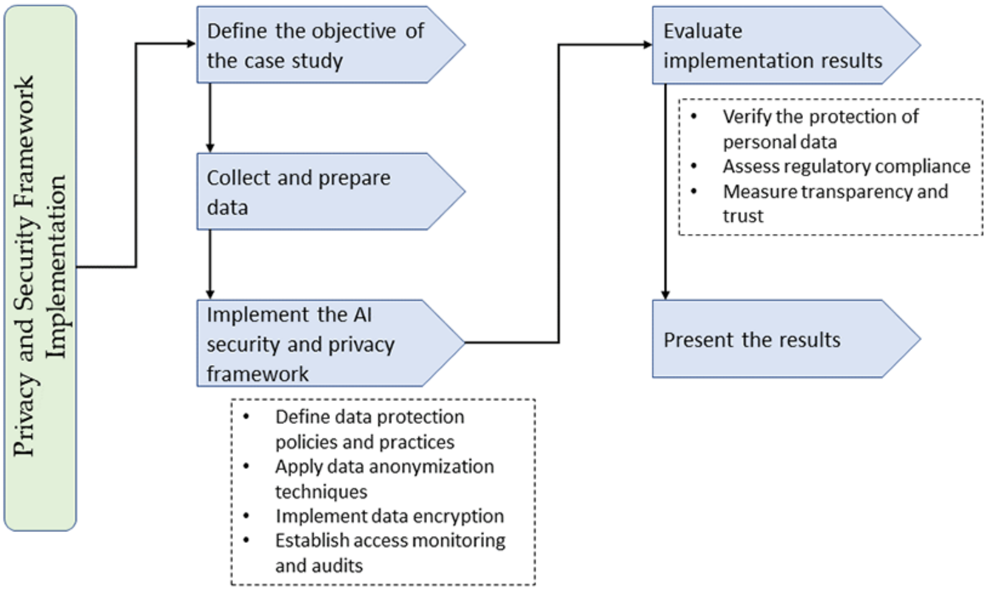
Privacy and Security Framework Implementation
Define the objective of the case study
Collect and prepare data
Implement the AI security and privacy framework
• Define data protection policies and practices
• Apply data anonymization techniques
• Implement data encryption
• Establish access monitoring and audits
Evaluate implementation results
• Verify the protection of personal data
• Assess regulatory compliance
• Measure transparency and trust
Present the results

Figure 2. AI security and privacy framework implementation flow.

In the evaluation phase of the implementation results, a thorough verification is carried out to protect personal data used in the facial recognition system, ensuring that these data are protected against unauthorized access and tampering. To this end, regulatory compliance has been assessed, provided that the framework complies with applicable data protection laws and regulations. In addition, transparency and trust have been measured by observing the perception of users and the public about the security and privacy of the facial recognition system.

In the results' presentation phase, the findings obtained are documented, including evidence of data protection, regulatory compliance, and improvement in transparency and trust. These results represent the impact and achievements derived from implementing the AI security and privacy framework in the case study of data protection in a facial recognition system. It is important to note that the results may vary depending on the context and the specific details of the implementation of the framework.

3.1. Data Sources

Table 2 contains the data used in the facial recognition system's case study on data protection. Each record in the table includes the following fields:

- ID: A unique identifier assigned to each record.
- Name: The name of the person associated with the record (it is not shown in the table to preserve data privacy).
- Age: The age of the person.
- Gender: The gender of the person, indicated as Female or Male.
- Biometric data: A series of numerical values representing biometric characteristics extracted from the face image (the values have been modified for presentation in the table).

These data are used in the case study to illustrate the development of a security and privacy framework in the context of a facial recognition system. It is important to note that the names, ages, genders, and images have been completely modified and do not correspond to accurate data.

Table 2. Biometric data considered in the case study.

ID	Age	Gender	Biometric Data
1	32	Female	0.85, 0.63, 0.45, 0.72
2	45	Male	0.76, 0.82, 0.69, 0.58
3	28	Female	0.72, 0.56, 0.91, 0.77
4	39	Male	0.65, 0.71, 0.82, 0.69
5	41	Female	0.68, 0.59, 0.74, 0.82
6	37	Male	0.79, 0.68, 0.56, 0.73
7	33	Female	0.74, 0.57, 0.85, 0.62
8	29	Male	0.61, 0.77, 0.68, 0.81
9	31	Female	0.67, 0.73, 0.64, 0.76
10	36	Male	0.73, 0.67, 0.78, 0.59
11	27	Female	0.84, 0.61, 0.47, 0.69
12	40	Male	0.77, 0.79, 0.71, 0.64
13	30	Female	0.63, 0.76, 0.59, 0.71
14	44	Male	0.69, 0.58, 0.75, 0.83
15	26	Female	0.71, 0.55, 0.92, 0.76
16	38	Male	0.64, 0.72, 0.83, 0.68
17	42	Female	0.67, 0.61, 0.76, 0.84
18	35	Male	0.83, 0.64, 0.42, 0.67
19	33	Female	0.78, 0.69, 0.57, 0.74
20	43	Male	0.75, 0.57, 0.84, 0.61

3.2. Algorithm Evaluation, Descriptive Statistics

Table 3 presents different statistics related to the variable of interest. The “Statistics” column indicates the type of statistics calculated for the variable, while the “Value” column shows the numerical results for each statistic. The statistics included in the table are the following:

- Minimum: Represents the minimum value recorded for the variable, which in this case is 20.
- Maximum: Indicates the maximum value registered for the variable, which is 50.
- Mean: Corresponds to the arithmetic mean of the values of the variable, approximately 34.89.
- Median: It is the central value of the data, which separates the lower half from the upper half. In this case, the median is 35.
- Standard deviation: Measures the spread of values around the mean. In this case, the standard deviation is approximately 6.13, indicating moderate variability in the data.

Table 3. Descriptive statistics of the collected data.

Statistics	Value
Minimum	20
Maximum	50
Half	34.89
Median	35
Standard deviation	6.13

These statistics provide a summary of the distribution and characteristics of the analyzed variable, which helps to understand its range, centrality, and dispersion.

Table 4 shows the evaluation metrics of the facial recognition model.

Table 4. Results of the evaluation of the facial recognition model.

Metrics	Value
Precision	0.92
Recall	0.88
Balanced precision	0.90
Confusion matrix:	
True positives	220
False positives	15
True negatives	950
False negatives	30

- Precision: The model is 92% accurate, which means that 92% of the optimistic predictions made by the model are correct. In other words, accuracy refers to the proportion of correctly recognized faces out of all optimistic predictions made.
- Recall: The recall of the model is 88%, which indicates that 88% of the people who should be identified (true positives) are correctly detected by the model.
- Balanced accuracy: Balanced accuracy is 90% and represents a measure of the performance of the proportional model. This metric is useful when there is an imbalance in the distribution of target classes and balances the importance of accuracy and recall.
- Confusion matrix: The confusion matrix shows the following results: 220 true positives, 15 false positives, 950 true negatives, and 30 false negatives were obtained.

Accuracy represents the total percentage of correct predictions, both positive and negative, in relation to all predictions made. In the context of evaluating a facial recognition model, accuracy would consider all correct and incorrect predictions, both correctly recognized faces and faces not correctly recognized. These results provide an overview of the performance of the evaluated facial recognition system after implementing the AI security framework.

Table 5 shows the privacy evaluation in the facial recognition system, considering different aspects related to the protection of sensitive data and the privacy of people.

Table 5. Evaluation of privacy in the facial recognition system.

Aspect	Evaluation
Data anonymization	Applied correctly
Information collection minimization	Complies with the principles of minimization
Protection of sensitive data	Security measures implemented
Compliance with regulations and standards	Complies with privacy regulations and standards

The table summarizes the evaluation of various privacy aspects in the facial recognition system. Specific measures have been taken to protect the privacy of individuals and the biometric data used in the system. The results obtained in each aspect evaluated are detailed below:

- Data anonymization: It has been verified that adequate data anonymization techniques have been applied, which indicates that the necessary measures have been taken to protect the identity of people in biometric data.
- Minimization of information collection: The system has been determined to comply with data minimization principles, which implies that only necessary information is collected, and the excessive or unnecessary collection of personal information is avoided.
- Protection of confidential data: Adequate security measures have been implemented to protect biometric data and other personal data stored in the system, which guarantees the protection of the privacy of individuals and the confidentiality of sensitive information.

- Compliance with regulations and standards: It has been verified that the system complies with established privacy regulations and standards, thus ensuring that the privacy rights of individuals are respected, and applicable legal and ethical requirements are met.

3.3. Data Retention Assessment

Table 6 presents detailed information on the retention of biometric data in the facial recognition system. Each record corresponds to a set of biometric data captured for a specific person. The fields in the table are described below:

- ID: Uniquely identifies each record, allowing for easy identification in the system database.
- Collection date: Indicates the date the biometric data were collected for each record.
- Retention date: This shows the date on which the data retention began, that is, when the period in which the data must be kept according to the established policies began.
- Deletion date: Indicates the date on which the secure deletion of the data will occur after the established retention period expires.

Table 6. Evaluation of data retention in the facial recognition system.

ID	Collection Date	Retention Date	Elimination Date
1	15 May 2022	15 May 2022	15 May 2027
2	2 August 2023	2 August 2023	2 August 2028
3	18 November 2024	18 November 2024	18 November 2029
4	7 March 2025	7 March 2025	7 March 2030
5	22 June 2026	22 June 2026	22 June 2031

These records help illustrate how the retention period of biometric data is recorded and tracked in the facial recognition system. Each entry in the table represents a different record in the system database, and compliance with established retention policies is guaranteed. This ensures that biometric data are retained appropriately and securely deleted once they are no longer needed.

The evaluation of data retention highlights compliance with good practices in the management and retention of biometric data in the facial recognition system. Appropriate measures are observed, such as setting an appropriate retention period, implementing policies for secure data deletion, and maintaining a detailed data retention and deletion record. These actions ensure that biometric data are treated responsibly and are securely disposed of once they are no longer needed, thus protecting the individual's privacy.

3.4. Evaluation of Accesses and Authorizations

The evaluation of access and authorizations in the facial recognition system analyzes how permissions and access are managed to ensure the security of sensitive data. Table 7 records the numbers of access made to the facial recognition system and evaluates whether the user who carried out the access has the corresponding authorization. Each entry is identified with a unique ID. The "User" column shows the email of the user who made the access. The column "Date and time of access" indicates the exact date and time when the access to the system was carried out. Finally, the "Authorized" column specifies whether the user has the appropriate permissions to access sensitive data.

When reviewing the access and authorization table, it is observed that the user "admin@example.com" has made two access attempts to the system, both authorized. Users "user1@example.com" and "user3@example.com" have also been granted privileged access to the system. On the other hand, the user "user2@example.com" tried to access the system, but his visa was not approved. These data provide insight into how access and authorizations are managed in the facial recognition system. The information of the users who access the system is recorded, and an authorization control is applied to allow access only to authorized users. This practice helps maintain the security of confidential data and detect possible security breaches by monitoring logged accesses.

Table 7. Evaluation of accesses and authorizations in the facial recognition system.

ID	User	Access Date and Time	Authorized
1	admin@example.com	15 May 2022 09:35:21	Yes
2	user1@example.com	16 May 2022 14:17:45	Yes
3	user2@example.com	16 May 2022 15:45:32	No
4	admin@example.com	17 May 2022 10:22:13	Yes
5	user3@example.com	18 May 2022 08:59:57	Yes

3.5. Data Quality Assessment

Table 8 presents various metrics for assessing biometric data quality in the facial recognition system. Each metric refers to a specific aspect, such as precision, reliability, and biases related to age, gender, and race. The "Value" column shows the results obtained for each evaluated metric.

Table 8. Evaluation of bias in the facial recognition system.

Metrics	Value
Precision	92.5%
Reliability	0.87
Age bias	0.02
Gender bias	0.05
Race bias	0.03

The accuracy, determined through verification tests, reached 92.5%, indicating the system's high capacity to identify people correctly. On the other hand, the reliability was evaluated with a coefficient of 0.87, showing good consistency in facial feature measurements over time. Biases related to age, gender, and race were measured using coefficients ranging from -1 to 1, where 0 indicates no discrimination. The values obtained reflect a minimal presence of bias, with an age bias of 0.02, a gender bias of 0.05, and a race bias of 0.03.

These data provide valuable information about the biometric data quality used in the facial recognition system. The high precision and reliability demonstrate the quality of the data. At the same time, the minimal presence of bias indicates that the system is designed to avoid unfair discrimination. These results support the efficacy and reliability of the facial recognition system by ensuring that the data used are reliable and reasonably representative of all individuals.

Evaluating the quality of the biometric data is essential to ensure the effectiveness and fairness of the facial recognition system. By verifying the accuracy and reliability of the data and addressing potential biases, it seeks to improve the accuracy of the identifications and prevent any form of unfair discrimination. This helps build confidence in the system and its ability to function fairly and accurately in different situations and with other groups of people.

The proposed framework for ensuring AI security and privacy encompasses multiple crucial aspects that interconnect and complement each other to provide a comprehensive assessment. The different evaluations carried out in this study focus on measuring various aspects of security and privacy, providing a holistic view of the AI system. While accuracy metrics are essential to assess facial recognition system performance, other equally critical dimensions must also be considered.

In the data protection assessment, the policies and practices implemented to safeguard the information used in the training of the AI model were analyzed. This evaluation revealed an adequate implementation of security measures to maintain the confidentiality and privacy of personal data. Data anonymization and encryption techniques were implemented to protect sensitive information from unauthorized access.

In addition, a data retention assessment was carried out, ensuring that biometric data were managed correctly, and policies were implemented for their secure deletion once no longer needed. This evaluation resulted in efficient data management, ensuring that data were not retained longer than required and minimizing the risk of improper access to sensitive information.

Another aspect evaluated was access control and authorizations. We reviewed the means of access to the facial recognition system and whether adequate controls were applied so as to limit access to sensitive data to authorized personnel only. Access auditing and monitoring helped detect potential security breaches and ensured a secure and trusted environment.

The biometric data quality was also evaluated, verifying their accuracy and reliability to guarantee fair and accurate results in the facial recognition system. This evaluation contributed to strengthening the model's reliability and minimizing biases that could affect the fairness and accuracy of the system.

These assessments complement and enrich each other, providing a comprehensive view of the AI system and its ability to ensure security and privacy. The specific results obtained in each evaluation are vital inputs for the proposed framework, allowing for the implementation of appropriate measures and the mitigation of risks in a broader context of AI. Integrating these metrics and results in the framework ensures a complete, ethical, and responsible approach toward developing and deploying AI systems that prioritize the security and privacy of users and society in general.

4. Discussion

Our framework has successfully met the challenge of safeguarding personal data and individual privacy. Through techniques such as anonymization and minimizing private information collection, we have reduced the exposure of sensitive data and ensured adequate privacy in the facial recognition system [38].

Regarding AI security, the framework has addressed the vulnerabilities and risks associated with AI systems. Implementing security frameworks has enabled the mitigating of possible attacks and malicious manipulations, providing an additional layer of protection to facial recognition systems [39]. Implementing access and authorization controls has limited access to sensitive data to authorized personnel only, preventing possible leaks or the misuse of information. In addition, security frameworks have been implemented to detect and mitigate possible attacks and malicious manipulations, such as image falsification or identity theft [40]. This has contributed to strengthening the reliability and integrity of the facial recognition.

Regarding confidence in the interpretation of models, the need to understand and explain the decisions made by AI models has been addressed. The interpretability of the models is crucial to guarantee understandable and justifiable results. We apply model interpretation and explainability techniques to improve our understanding of how specific predictions and decisions are generated.

The framework has shown promising results regarding data protection, security, privacy, and biometric data quality in the facial recognition system. Robust policies and practices have been implemented to safeguard data used in AI model training [41]. Furthermore, the implementation of data encryption and access controls has provided an additional layer of security, protecting data both in transit and at rest [42]. It is also important to note that we have carried out a thorough and objective evaluation of the accuracy and reliability of the biometric data used in the facial recognition system. The results obtained, such as an accuracy of 92.5% and a reliability of 0.87, are evidence of the high quality and consistency of the biometric data. In addition, we have carried out a detailed analysis of possible biases, such as those related to age, gender, and race, to ensure that the system does not show preferences or discrimination toward any group and to ensure fairness in its operation.

Security in the context of AI encompasses multiple crucial aspects that need to be addressed holistically to ensure the trust and reliability of AI systems. Our framework addresses three fundamental dimensions of security in AI: the security of training data, the security of the model, and confidence in the model's interpretation. By addressing these dimensions, our framework presents itself as a comprehensive solution ensuring data protection, models, and performance in AI systems. These aspects are essential to promote trust and the responsible adoption of AI in various fields, from facial recognition to other critical applications in our society.

5. Conclusions

During the development of this work, we explored various aspects related to the security and privacy of AI. The importance of protecting the data used to train AI models has been emphasized, and policies and practices have been analyzed to safeguard the confidentiality of sensitive data. Vulnerabilities and security risks in AI systems have also been addressed, along with potential threats and malicious manipulations that may arise.

In addition, emphasis has been placed on the privacy challenges associated with AI, and approaches such as data anonymization and minimizing the collection of personal information have been explored to protect individual privacy in AI systems.

It is essential to develop and adopt robust frameworks to ensure the security and privacy of AI. These frameworks provide guidance and best practices to protect data, mitigate security risks, and preserve individual privacy. By implementing these frameworks, we can encourage the responsible, ethical, and trustworthy use of AI, building trust among users and stakeholders.

However, it is essential to note that new challenges in AI security and privacy are constantly evolving. We face new challenges and risks as technology advances and new scenarios and applications emerge. Therefore, staying current, monitoring emerging insights, and researching and developing solutions to address these evolving challenges is crucial.

In addition, addressing these issues comprehensively and collaboratively is essential. Governments, organizations, researchers, and society at large must work together to establish solid regulatory frameworks, promote ethical standards, and raise the awareness of the importance of AI security and privacy. By protecting data, mitigating security risks, and preserving individual privacy, we can harness the power of AI responsibly and ethically.

Author Contributions: Conceptualization, W.V.-C. and J.G.-O.; methodology, W.V.-C.; software, J.G.-O.; validation, W.V.-C.; formal analysis, W.V.-C.; investigation, J.G.-O.; data curation, W.V.-C. and J.G.-O.; writing—original draft preparation, J.G.-O.; writing—review and editing, W.V.-C.; visualization, J.G.-O.; supervision, W.V.-C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data used in this study were obtained from sources of the university participating in the study. However, it is essential to note that the implemented source code for deep learning models is not publicly available due to intellectual property and copyright restrictions. Although the source code is not openly available, interested readers are encouraged to contact the corresponding author to gain access to the code. To request the source code, please send an email to william.villegas@udla.edu.ec. The author commits to making the code available to interested readers to foster collaboration and knowledge sharing in drought forecasting and deep learning.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kieslich, K.; Keller, B.; Starke, C. Artificial Intelligence Ethics by Design. Evaluating Public Perception on the Importance of Ethical Design Principles of Artificial Intelligence. *Big Data Soc.* **2022**, *9*, 20539517221092956. [CrossRef]
2. Sun, L.; Sun, L.; Jiang, X.; Ren, H.; Ren, H.; Guo, Y. Edge-Cloud Computing and Artificial Intelligence in Internet of Medical Things: Architecture, Technology and Application. *IEEE Access* **2020**, *8*, 101079–101092. [CrossRef]

3. Zhu, T.; Ye, D.; Wang, W.; Zhou, W.; Yu, P.S. More Than Privacy: Applying Differential Privacy in Key Areas of Artificial Intelligence. *IEEE Trans. Knowl. Data Eng.* **2022**, *34*, 2824–2843. [CrossRef]
4. Cavus, N.; Mohammed, Y.B.; Gital, A.Y.; Bulama, M.; Tukur, A.M.; Mohammed, D.; Isah, M.L.; Hassan, A. Emotional Artificial Neural Networks and Gaussian Process-Regression-Based Hybrid Machine-Learning Model for Prediction of Security and Privacy Effects on M-Banking Attractiveness. *Sustainability* **2022**, *14*, 5826. [CrossRef]
5. Chatterjee, S.; Ghosh, S.K.; Chaudhuri, R.; Chaudhuri, S. Adoption of AI-Integrated CRM System by Indian Industry: From Security and Privacy Perspective. *Inf. Comput. Secur.* **2020**, *29*, 1–24. [CrossRef]
6. Almalawi, A.; Khan, A.I.; Alsolami, F.; Abushark, Y.B.; Alfakeeh, A.S.; Mekuriyaw, W.D. Analysis of the Exploration of Security and Privacy for Healthcare Management Using Artificial Intelligence: Saudi Hospitals. *Comput. Intell. Neurosci.* **2022**, *2022*, 4048197. [CrossRef]
7. Oumaima, F.; Karim, Z.; Abdellatif, E.G.; Mohammed, B. A Survey on Blockchain and Artificial Intelligence Technologies for Enhancing Security and Privacy in Smart Environments. *IEEE Access* **2022**, *10*, 93168–93186. [CrossRef]
8. Al-Rubaie, M.; Chang, J.M. Privacy-Preserving Machine Learning: Threats and Solutions. *IEEE Secur. Priv.* **2019**, *17*, 49–58. [CrossRef]
9. Shokri, R.; Stronati, M.; Song, C.; Shmatikov, V. Membership Inference Attacks Against Machine Learning Models. In Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA, 22–26 May 2017.
10. Dwork, C. Differential Privacy: A Survey of Results. In *Theory and Applications of Models of Computation*; Agrawal, M., Du, D., Duan, Z., Li, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 1–19.
11. Lindell, Y.; Pinkas, B.; Smart, N.P.; Yanai, A. Efficient Constant-Round Multi-Party Computation Combining BMR and SPDZ. *J. Cryptol.* **2019**, *32*, 1026–1069. [CrossRef]
12. Bonawitz, K.; Eichner, H.; Grieskamp, W.; Huba, D.; Ingerman, A.; Ivanov, V.; Kiddon, C.; Konečný, J.; Mazzocchi, S.; McMahan, B.; et al. Towards Federated Learning at Scale: System Design. In Proceedings of the Machine Learning and Systems, MLSys 2019, Stanford, CA, USA, 31 March–2 April 2019; Volume 1, pp. 374–388.
13. Almalawi, A.; Khan, A.I.; Alsolami, F.; Abushark, Y.B.; Alfakeeh, A.S. Managing Security of Healthcare Data for a Modern Healthcare System. *Sensors* **2023**, *23*, 3612. [CrossRef]
14. Tanuwidjaja, H.C.; Choi, R.; Baek, S.; Kim, K. Privacy-Preserving Deep Learning on Machine Learning as a Service-a Comprehensive Survey. *IEEE Access* **2020**, *8*, 167425–167447. [CrossRef]
15. Canbay, Y.; Sağıroğlu, S. Big Data Anonymization with Spark. In Proceedings of the 2017 International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 5–8 October 2017; pp. 833–838.
16. Marinos, L. Risk Management and Risk Assessment at ENISA: Issues and Challenges. In Proceedings of the First International Conference on Availability, Reliability and Security, ARES 2006, Vienna, Austria, 20–22 April 2006; Volume 2006, pp. 2–3.
17. Lecuyer, M.; Atlidakis, V.; Geambasu, R.; Hsu, D.; Jana, S. Certified Robustness to Adversarial Examples with Differential Privacy. In Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 19–23 May 2019.
18. Hlávka, J.P. Security, Privacy, and Information-Sharing Aspects of Healthcare Artificial Intelligence. In *Artificial Intelligence in Healthcare*; Elsevier: Amsterdam, The Netherlands, 2020.
19. Michael, J.B. Security and Privacy for Edge Artificial Intelligence. *IEEE Secur. Priv.* **2021**, *19*, 4–7. [CrossRef]
20. Machin, J.; Batista, E.; Martínez-Ballesté, A.; Solanas, A. Privacy and Security in Cognitive Cities: A Systematic Review. *Appl. Sci.* **2021**, *11*, 4471. [CrossRef]
21. Chung, K.C.; Chen, C.H.; Tsai, H.H.; Chuang, Y.H. Social Media Privacy Management Strategies: A SEM Analysis of User Privacy Behaviors. *Comput. Commun.* **2021**, *174*, 122–130. [CrossRef]
22. Fidas, C.A.; Lyras, D. A Review of EEG-Based User Authentication: Trends and Future Research Directions. *IEEE Access* **2023**, *11*, 22917–22934. [CrossRef]
23. Al-Ghamdi, L.M. Towards Adopting AI Techniques for Monitoring Social Media Activities. *Sustain. Eng. Innov.* **2021**, *3*, 15–22. [CrossRef]
24. Saura, J.R.; Ribeiro-Soriano, D.; Palacios-Marqués, D. Assessing Behavioral Data Science Privacy Issues in Government Artificial Intelligence Deployment. *Gov. Inf. Q.* **2022**, *39*, 101679. [CrossRef]
25. Yu, H.; Guo, Y. Generative Artificial Intelligence Empowers Educational Reform: Current Status, Issues, and Prospects. *Front. Educ.* **2023**, *8*, 1183162. [CrossRef]
26. Rieder, E.; Schmuck, M.; Tugui, A. A Scientific Perspective on Using Artificial Intelligence in Sustainable Urban Development. *Big Data Cogn. Comput.* **2023**, *7*, 3. [CrossRef]
27. Chen, Y.; Shen, C.; Wang, Q.; Li, Q.; Wang, C.; Ji, S.; Li, K.; Guan, X. Security and Privacy Risks in Artificial Intelligence Systems. *Jisuanji Yanjiu Yu Fazhan/Comput. Res. Dev.* **2019**, *56*, 2135–2150.
28. Smith, M.; Miller, S. The Ethical Application of Biometric Facial Recognition Technology. *AI Soc.* **2022**, *37*, 167–175. [CrossRef] [PubMed]
29. Li, X.; Zhang, T. An Exploration on Artificial Intelligence Application: From Security, Privacy and Ethic Perspective. In Proceedings of the 2017 2nd IEEE International Conference on Cloud Computing and Big Data Analysis, ICCCBDA 2017, Chengdu, China, 28–30 April 2017.
30. Li, C.S.; Wang, S.Y.; Li, Y.M.; Zhang, C.Z.; Yuan, Y.; Wang, G.R. Survey on Reverse-Engineering Artificial Intelligence. *Ruan Jian Xue Bao/J. Softw.* **2023**, *34*, 712–732. [CrossRef]

31. Wang, Z.; Zhang, Y.; Cao, J.; Hou, R.; Lu, J. The Application of Privacy Protection and Artificial Intelligence Technology in the Information Auxiliary System of the Prevention and Control of COVID-19. *Chin. J. Med. Sci. Res. Manag.* **2020**, *33*, E011.
32. Wang, Y.; Su, Z.; Zhang, N.; Xing, R.; Liu, D.; Luan, T.H.; Shen, X. A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 319–352. [CrossRef]
33. Bandi, A.; Yalamarthi, S. Towards Artificial Intelligence Empowered Security and Privacy Issues in 6G Communications. In Proceedings of the International Conference on Sustainable Computing and Data Communication Systems, ICSCDS 2022, Erode, India, 7–9 April 2022.
34. Liu, Q.; Wang, G.; Hu, J.; Wu, J. Preface of Special Issue on Artificial Intelligence: The Security & Privacy Opportunities and Challenges for Emerging Applications. *Future Gener. Comput. Syst.* **2022**, *133*, 169–170.
35. Al-Khassawneh, Y.A. A Review of Artificial Intelligence in Security and Privacy: Research Advances, Applications, Opportunities, and Challenges. *Indones. J. Sci. Technol.* **2023**, *8*, 79–96. [CrossRef]
36. Onyema, E.M.; Dalal, S.; Romero, C.A.T.; Seth, B.; Young, P.; Wajid, M.A. Design of Intrusion Detection System Based on Cyborg Intelligence for Security of Cloud Network Traffic of Smart Cities. *J. Cloud Comput.* **2022**, *11*, 26. [CrossRef]
37. Ren, K.; Meng, Q.; Yan, S.; Qin, Z. Survey of Artificial Intelligence Data Security and Privacy Protection. *Chin. J. Netw. Inf. Secur.* **2021**, *7*, 1–10. [CrossRef]
38. Zhu, J.; Wu, J.; Bashir, A.K.; Pan, Q.; Yang, W. Privacy-Preserving Federated Learning of Remote Sensing Image Classification With Dishonest Majority. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.* **2023**, *16*, 4685–4698. [CrossRef]
39. Deebak, B.D.; AL-Turjman, F. Privacy-Preserving in Smart Contracts Using Blockchain and Artificial Intelligence for Cyber Risk Measurements. *J. Inf. Secur. Appl.* **2021**, *58*, 102749. [CrossRef]
40. Kim, S.K.; Huh, J.H. Artificial Neural Network Blockchain Techniques for Healthcare System: Focusing on the Personal Health Records. *Electronics* **2020**, *9*, 763. [CrossRef]
41. Jabbarpour, M.R.; Saghiri, A.M.; Sookhak, M. A Framework for Component Selection Considering Dark Sides of Artificial Intelligence: A Case Study on Autonomous Vehicle. *Electronics* **2021**, *10*, 384. [CrossRef]
42. Himeur, Y.; Sohail, S.S.; Bensaali, F.; Amira, A.; Alazab, M. Latest Trends of Security and Privacy in Recommender Systems: A Comprehensive Review and Future Perspectives. *Comput. Secur.* **2022**, *118*, 102746. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.