future internet

IMPACT FACTOR 2.8

CITESCORE 7.1

Review

Opportunities and Challenges of Artificial Intelligence Applied to Identity and Access Management in Industrial Environments

Jesús Vegas and César Llamas

MDPI

https://doi.org/10.3390/fi16120469

future internet

MDPI

Review

Opportunities and Challenges of Artificial Intelligence Applied to Identity and Access Management in Industrial Environments

Jesús Vegas * and César Llamas

Escuela de Ingeniería Informática, Universidad de Valladolid, Paseo de Belén 15, 47011 Valladolid, Spain; cesar.llamas@uva.es

* Correspondence: jvegas@uva.es; Tel.: +34-983-185608

Abstract: The integration of artificial intelligence(AI) technologies into identity and access management (IAM) systems has greatly improved access control and management, offering more robust, adaptive, and intelligent solutions than traditional methods. AI-driven IAM systems enhance security, operational efficiency, and introduce new capabilities in industrial environments. In this narrative review, we present the state-of-the-art AI technologies in industrial IAM, focusing on methods such as biometric, comprising facial and voice recognition, and multifactor authentication for robust security. It addresses the challenges and solutions in implementing AI-based IAM systems in industrial settings, including security, privacy, evaluation, and continuous improvement. We present also the emerging trends and future directions, highlighting AI's potential to transform industrial security measures. This review aims to guide researchers and practitioners in developing and implementing next-generation access control systems, proposing future research directions to address challenges and optimize AI applications in this domain.

Keywords: identity and access management; artificial intelligence; industrial environments

Citation: Vegas, J.; Llamas, C. Opportunities and Challenges of Artificial Intelligence Applied to Identity and Access Management in Industrial Environments. *Future Internet* **2024**, *16*, 469. https://doi.org/10.3390/fi16120469

Academic Editor: Gianluigi Ferrari

Received: 4 October 2024
Revised: 13 December 2024
Accepted: 13 December 2024
Published: 16 December 2024

1. Introduction

The irruption of artificial intelligence (AI) is transforming how we interact with technology, and the industrial sector is no exception. AI has infiltrated all aspects of our lives, from communication to work processes. In the industrial sector, AI plays a crucial role in enhancing security, efficiency, and automation [1].

Within this context, the industrial sector is increasingly adopting AI-driven identity and access management (IAM) systems to improve access control and management. Traditional IAM methods, while effective to a degree, often fall short in addressing the dynamic and complex security needs of modern industrial environments [2]. AI technologies offer adaptive, intelligent solutions that can significantly enhance the robustness and efficiency of IAM systems.

AI is particularly impactful in several key areas:

- Cybersecurity AI is used to detect and respond to cyber threats, identify vulnerabilities, and monitor industrial networks in real-time [3].
- Operational Safety AI improves safety and accident prevention by monitoring working conditions, predicting equipment failures, and assessing operational risks [4].
- Supply Chain Security AI applications include monitoring and tracking goods, verifying suppliers, and preventing theft and loss [5].
- Industrial Automation AI enhances safety in automation, ensuring safety in collaborative robots, implementing intelligent emergency stop systems, and simulating risk scenarios [6].
- Industry 4.0 and IIoT AI secures IoT devices, manages identities and access, and secures communications between industrial devices and systems [7].

IAM systems are essential for ensuring the security and integrity of industrial facilities, protecting critical assets, and preventing unauthorized access [2]. AI is understood as a collection of technologies, including machine learning (ML), deep learning (DL), and data analytics, which are designed to improve decision-making, enhance security, and automate processes within IAM systems. Integrating AI technologies into IAM enhances security measures, improves operational efficiency, and enables new capabilities [8].

AI-based IAM systems are becoming essential for ensuring robust data security and governance across organizations, with market forecasts indicating a rising demand for these technologies. According to the report [9], the global identity and access management market size was valued at USD 15.93 billion in 2022 and is projected to expand at a compound annual growth rate (CAGR) of 12.6% from 2023 to 2030. As such, AI-based IAM systems are expected to grow in importance and adoption in the coming years.

A systematic review of the literature conducted by Alomari et al. [10] from 2016 to 2021 highlights the growing focus on AI's role in IAM, with a significant body of work exploring its potential. This review lays a foundation for further research into AI's integration with IAM and its future developments.

This paper reviews the current state-of-the-art AI technologies and their applications in industrial IAM. From an initial review of the differences between IAM systems in industrial environments and general ones, we delve into the technologies and algorithms that are driving the advancements in this field.

Although several research initiatives have driven the deployment of AI solutions in the context of IAM systems, there are difficulties in assessing the real impact of this research, as companies often do not publish the outcome of such application. Due to the lack of sufficient evidence of successful industrial applications of AI in IAM systems, industrial adoption of the technology may be being mitigated.

Furthermore, based on this assessment, the objective of our research is to propose a strategic road map to guide both researchers and manufacturers in the transition towards the integration of AI in industrial IAM systems, so the following research questions were formulated:

RQ1: What are the main contributions of AI in identification and authentication with application in industrial IAM systems?
RQ2: What are the advanced capabilities that AI can bring to IAM systems?
RQ3: What are the main challenges and future lines of research?

To answer these questions, we start by identifying the main requirements of IAM systems, especially in industrial environments. Then, we explore various AI-driven methods, including computer vision for facial recognition, biometric authentication, and multifactor authentication (MFA), highlighting their capabilities in providing robust identification and authentication solutions. We also discuss the advanced capabilities that AI brings to IAM systems and how these capabilities enhance security and operational efficiency in industrial environments. Furthermore, emerging trends and future directions in AI applications for industrial IAM are also discussed, providing insights into the potential of AI to transform security measures in industrial settings. Finally, this article also shows as conclusion the benefits and challenges in implementing AI-based IAM systems.

In order to carry out this comprehensive review, our methodology involved the following steps. Firstly, a literature search on academic databases was conducted using carefully selected keywords relevant to the research questions such as "artificial intelligence in industrial identity management", "authentication in industrial settings", among others, ensuring that the selected studies were directly applicable to the subject matter. These sources are recognized for their relevance to industrial cybersecurity and identity management issues. This allowed us to identify a wide range of peer-reviewed articles, conference papers, and other credible sources. Secondly, inclusion and exclusion criteria were applied to ensure that only high-quality, relevant studies were selected. In our review, we included studies that specifically address the application of AI techniques in identity and access management (IAM), focusing primarily on peer-reviewed journal articles and conference

papers published within the last 10 years. However, some older papers were included due to their relevance. The selected papers discuss AI-driven methods such as machine learning, anomaly detection, and automated decision-making in the context of IAM security. Articles not focused on AI or IAM, outdated technologies, non-peer-reviewed sources, and duplicate studies were excluded. The identified studies were evaluated according to their relevance, methodology, and scientific contribution, focusing on practical solutions for authentication and identity management in industry. This process aimed to eliminate bias and focus on the most pertinent research to address our research questions. Finally, the synthesis and analysis of the identified studies was conducted, comparing, contrasting, and identifying trends, gaps, and areas of consensus or disagreement in the literature. The information extracted and the corresponding articles were then organized according to different categories related with the research questions trying to identify the main requirements, use of AI technologies, advanced capabilities, trends, and challenges in the field of industrial IAM systems. This methodology ensures that the review covers the most current and relevant solutions, highlighting innovations and challenges in implementing IAM systems in industrial environments.

Table A1 is provided in the Appendix A to offer a clearer overview of the reviewed works. This table summarizes the application domain, objectives, methodologies, and strengths of the reviewed articles, offering readers a concise snapshot to better understand the scope and contributions of each study.

This paper is organized as follows: Section 2 describes the importance of identity and access management in industrial environments; Section 3 presents the role of AI technologies in identification and authentication; Section 4 discusses the advanced capabilities of AI-based IAM systems; Section 5 outlines future research directions in AI applications for IAM in industrial environments; Section 6 synthesizes and critically evaluates the key findings from the literature review; and Section 7 summarizes the main findings and conclusions of the conducted research, answering the research questions stated above. Finally, the Appendix A provides a summary of the reviewed works.

2. Background

Identity and access management (IAM) is a critical component for maintaining security within industrial environments, which include factories, power plants, and other critical infrastructure. These settings require stringent security measures to safeguard both physical and digital assets. IAM systems are crucial for controlling who has access to various parts of an industrial facility and ensuring that only authorized personnel can perform specific tasks. IAM involves processes, policies, and technologies that ensure the right individuals have access to the right resources at the right times for the right reasons.

Traditional IAM methods often rely on static rules and manual oversight, which can be inadequate against evolving security threats and the increasing complexity of industrial operations. One of the main challenges in industrial environments is managing access to a wide range of resources, including physical assets, digital systems, and data. This requires a comprehensive IAM system capable of handling the complexity and scale of industrial operations while ensuring security and regulatory compliance.

IAM systems in industrial environments must accommodate both IT and OT (operational technology) integration, which requires managing access across traditional IT infrastructure and specialized OT systems. This environment necessitates real-time access control and anomaly detection due to the potential impact on production and safety, which differs from general IAM systems typically focused on standard IT environments. Furthermore, industrial IAM must be scalable and flexible to manage a wide range of devices, from sensors to complex machinery, which contrasts with general IAM solutions that primarily focus on user-based access rather than extensive device-level interoperability.

IAM systems in industrial environments must address several key requirements, including the following:

- User Management and Authentication: In industrial IAM systems, centralized and distributed user management authentication models offer distinct advantages and limitations. Centralized models simplify user management and control through a single authentication server, which efficiently oversees access, enables single sign-on (SSO), and streamlines policy enforcement across systems. However, they are prone to single points of failure and potential security vulnerabilities due to centralized data handling [11]. Distributed authentication, increasingly enabled by blockchain, mitigates these risks by distributing trust and authentication tasks across a network, reducing the chance of total system failure while enhancing data privacy and scalability. Blockchain-based models, like RC-AAM, avoid central dependency and enable decentralized role-centric authentication, enhancing security in industrial and IoT settings [12]. While distributed models offer robustness and fault tolerance, they often demand higher technical complexity and infrastructure to implement effectively, highlighting a trade-off between centralized simplicity and distributed resilience.
- Access Control: Industrial IAM systems employ various access control models tailored to the complexity and security requirements of industrial environments. Role-based access control (RBAC), adapted with node-based and hierarchical features, remains foundational due to its simplicity in managing roles across different users [13]. Attribute-based access control (ABAC) adds flexibility by using device and user attributes, making it effective for systems like programmable logic controllers (PLCs) [14]. Multi-granularity models are also applied in Industry 4.0 settings to adjust access across product life cycles, improving management efficiency [15]. Additionally, task–role-based access control (T-RBAC) aligns permissions with specific tasks, adding another layer of role differentiation [16], and context-aware access control adapts permissions dynamically based on environmental factors, enhancing security in real-time industrial operations [17]. Together, these models create a layered security approach for managing diverse access needs in industrial systems.
- Enhanced Security: IAM systems in industrial contexts enhance security by enforcing unified policies across various platforms, addressing both access control and data protection through multiple layers of security measures. By centralizing authentication, authorization, and role management, IAM reduces the risk of unauthorized access by maintaining consistent security protocols that prevent data breaches, especially in cloud or multi-platform environments [18]. Furthermore, IAM frameworks, when optimized, can detect and minimize unnecessary permissions that could be exploited, thereby reducing the risk of insider threats and external attacks [19]. These systems also ensure that security policies dynamically adapt to changing network conditions, protecting industrial systems from unauthorized data flow across diverse trust domains [20]. Ultimately, IAM enforces security policies with both efficiency and adaptability, strengthening the industrial environment's resilience to cyber threats.

At the same time, industrial IAM systems play a vital role in ensuring regulatory compliance by providing detailed access logs and audit trails, which are essential for meeting industry standards and legal requirements [21]. In addition to compliance, these systems help reduce operational costs by automating access control processes, minimizing manual interventions, and lowering help desk demands [22–24]. They also offer self-service functionalities, enabling users to manage their own access rights, which lightens the load on IT staff [22].

To keep pace with the expanding complexity and scale of industrial environments, IAM systems must provide scalability and performance, supporting a growing number of users, devices, and applications with high reliability [18,24]. Finally, effective IAM solutions ensure integration with other systems, harmonizing data and improving security by analyzing identity and access information across platforms, which enhances both operational efficiency and overall security [2,25].

IAM plays a pivotal role in industrial environments by centralizing user management, enhancing security, improving efficiency, and ensuring compliance. The integration of IAM

with other systems and the use of RBAC further strengthen its effectiveness. As industrial environments continue to evolve, the importance of robust and scalable IAM systems will increase, making them indispensable for maintaining security and operational efficiency.

All this has been represented in the schematic of Figure 1, which comprised the main components of an IAM system. It shows how the identity manager subsystem (Figure 1b) deals with the identities associated through the identification and authentication mechanisms (Figure 1a) distributed throughout the industrial environment. The access manager subsystem (Figure 1d) grants or denies a user access to a specific component of the industrial environment (Figure 1e), be it production, management, or business, based on the information stored in the IAM system. The system database (Figure 1c) centrally maintains model, policy, audit, and log data through an appropriate front-end and back-end platform.

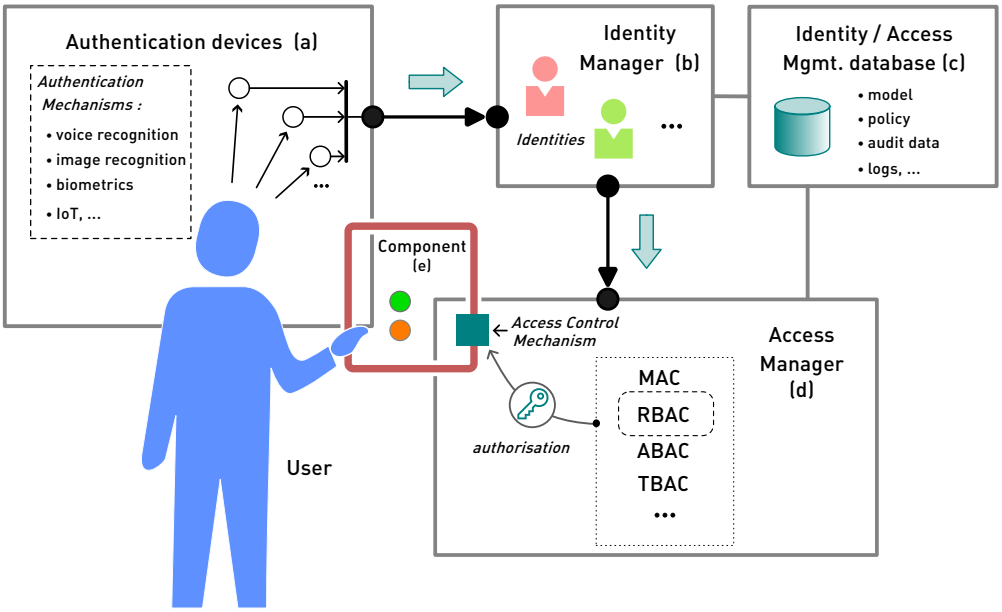

Figure 1. Overview of an IAM system and main components of an identity and access management system in relation to an industrial environment [2,25,26]. (Figure developed by the authors.)

The integration of artificial intelligence (AI) into IAM systems has transformed how access is controlled and managed, offering more robust, adaptive, and intelligent solutions compared to traditional methods. This state-of-the-art review explores current advancements in AI applications for IAM in industrial settings, highlighting key technologies, methodologies, and their impacts on industrial security. The focus is on integrating AI technologies such as machine learning, computer vision, and biometric recognition into IAM systems, as well as the advanced capabilities that AI brings, including real-time monitoring, anomaly detection, and predictive analytics.

3. AI-Based Identification and Authentication

A critical capability of IAM infrastructure is user identification and authentication and that is the motivation to set the first research question, as follows: What are the main contributions of AI in identification and authentication with application in industrial IAM systems?

As a result of the literature review, in this section, we present the main AI capabilities applied in identification and authentication processes in industrial IAM systems. These are pivoting around biometric recognition reinforced by the use of deep learning algorithms, which are essential for enhancing the accuracy, reliability, and versatility of IAM systems in industrial environments.

3.1. Biometric Recognition

Biometric recognition systems have gained significant traction in industrial environments due to their high accuracy and reliability. Biometric recognition uses unique physical or behavioral characteristics, such as fingerprints, facial features, or iris patterns, to authenticate users [27]. AI-driven biometric systems leverage deep learning algorithms to enhance the accuracy and robustness of biometric matching, even in challenging industrial conditions [28,29].

AI-powered facial recognition systems analyze facial features and match them against a database of known individuals, offering high accuracy and speed. These systems are ideal for industrial IAM applications such as access control, attendance tracking, and security monitoring [30].

These advancements extend beyond facial recognition to other biometric modalities such as fingerprint, iris, and voice recognition, making AI-driven systems versatile and highly reliable [31].

Voice recognition systems use AI algorithms to analyze voice patterns and authenticate users based on their unique vocal characteristics. Voice recognition provides a hands-free and secure authentication method, ideal for industrial environments where users may have limited mobility or need to access systems while performing other tasks [32,33].

3.2. Enhanced Accuracy Through Deep Learning

Deep learning algorithms, a subset of machine learning, are pivotal in improving the accuracy of biometric systems. These algorithms process vast amounts of data, learning intricate patterns and features critical for accurate biometric recognition. Convolutional neural networks (CNNs) have been extensively used for facial recognition, significantly improving the system's ability to correctly identify individuals even with variations in lighting, angles, and expressions [34]. This capability is crucial in industrial settings where environmental conditions can be unpredictable.

Deep learning's effectiveness in enhancing biometric systems is demonstrated through various studies. For example, deep learning combined with serial fusion methods significantly improves authentication accuracy, achieving an AUC of 0.9996 [35]. Another study reviews over 120 works on biometric recognition using deep learning models, demonstrating substantial improvements in accuracy across face, fingerprint, and iris recognition [36].

In industrial applications, a method combining machine vision and deep learning for quality control achieves high accuracy with limited computational time using low-cost hardware [37]. Additionally, a comparative study of single-mode, two-mode, and three-mode biometric systems using CNNs and genetic algorithms shows that three-mode systems significantly outperform others in terms of accuracy and robustness [38].

At the same time, the behavioral biometrics leverages AI to analyze patterns in human activities such as typing, walking, and using devices, enhancing security by providing continuous and unobtrusive authentication. AI algorithms process vast amounts of behavioral data, identifying unique traits and detecting anomalies that suggest potential security threats. This technology is particularly effective because it adapts to changes in user behavior over time, improving accuracy and robustness against fraud. Recent studies highlight AI's role in refining these systems, showing significant improvements in both identification accuracy and user experience [39–41].

3.3. Robustness in Challenging Conditions

In industrial environments, biometric systems must contend with various challenges such as dust, noise, vibrations, and extreme temperatures. Lawton [42] discusses the environmental and security challenges associated with biometric systems, providing insights into how these challenges can be addressed to enhance the reliability and robustness of biometric technologies.

French et al. [43] examine the application of microsystems in harsh environments, including high temperatures, chemical disturbances, electromagnetic noise, and mechan-

ical vibrations. They discuss the additional challenges these conditions present and the multidisciplinary approaches required to overcome them.

Gawande et al. [44] discuss various challenges in designing biometric-based security systems, including environmental factors such as noise and non-ideal conditions, and propose feature extraction approaches to enhance robustness and accuracy.

Ross et al. [45] address the problem of noisy sensor data and other environmental challenges in biometric verification systems. They explore how multimodal biometric systems, which combine multiple sources of biometric evidence, can improve performance in challenging conditions.

AI enhances the robustness of biometric systems in challenging conditions. Deep learning algorithms can adapt and perform consistently under such conditions [46]. For instance, in environments where fingerprint quality might be degraded due to dirt or damage, deep learning models can still accurately match fingerprints by focusing on deeper, more stable features rather than superficial ones [47].

Nguyen et al. [48] present a study on iris recognition in varying lighting conditions, demonstrating the robustness of deep learning models in adapting to challenging environments. The study shows that deep learning models can maintain high accuracy even under varying lighting conditions, unlike traditional algorithms that struggle in such scenarios.

3.4. Multifactor Authentication (MFA)

Multifactor authentication (MFA) leverages AI to enhance security by combining multiple authentication factors, such as passwords, biometrics, and one-time passcodes. AI algorithms can analyze these factors in real-time to detect anomalies and prevent unauthorized access attempts. MFA provides an additional layer of security, reducing the risk of credential theft and unauthorized access in industrial environments [49].

4. Advanced Capabilities in AI-Based IAM Systems

In the previous section we have discussed the main AI technologies used in identification and authentication processes in industrial IAM systems. In this section, we delve into the advanced capabilities that AI brings to IAM systems by focusing our literature review on answering the second research question: What are the advanced capabilities that AI can bring to IAM systems?

As a result of this review, we found that the advanced capabilities of AI-based IAM systems in industrial environments comprise real-time monitoring, anomaly detection, and predictive analytics. These capabilities are essential for enhancing security, improving operational efficiency, and enabling new functionalities in industrial environments.

4.1. Anomaly Detection and Real-Time Monitoring

Anomaly detection and real-time monitoring are key capabilities of AI-based IAM systems. Machine learning algorithms excel at detecting anomalies by learning normal behavior patterns of users and devices. In industrial settings, ML models can continuously monitor access logs, network traffic, and user behavior to identify deviations from the norm that may indicate security breaches or unauthorized access attempts. This proactive approach helps in identifying and mitigating security threats before they can cause significant harm [50]. For instance, ML-based systems can detect unusual login times, access from unrecognized devices, or attempts to access restricted areas, enabling rapid response to potential threats [51].

Regarding this, several studies have investigated the use of machine learning algorithms for anomaly detection in industrial environments. Notably, the following studies stand out.

Liu et al. propose a system called MLTracer that uses unsupervised learning to detect anomalies in user logins, identifying suspicious activities in real-time [52]. Tian et al. present a machine-learning-based anomaly detection method for host-based intrusion detection systems, utilizing shell command sequences to characterize user behavior [53]. Hosic et al.

propose using genetic programming to evolve decision trees for detecting anomalies in industrial control system networks [54]. Saha et al. introduce Quantile LSTM for detecting anomalies in industrial time-series data [55]. Sharma et al. present KDetect, an unsupervised anomaly detection algorithm for cloud systems using time series clustering [56]. Zheng et al. propose a hybrid clustering-PSO algorithm for anomaly intrusion detection, combining unsupervised clustering with particle swarm optimization [57].

4.2. Predictive Analytics

Predictive analytics is another key capability of AI-based IAM systems, helping forecast potential security incidents by analyzing historical access data. This capability is crucial in industrial environments where the consequences of security breaches can be severe. ML can analyze historical access patterns to predict potential security incidents, allowing organizations to anticipate and mitigate risks before they escalate into serious security breaches. For example, ML algorithms can identify trends in access requests and predict when and where unauthorized access attempts are likely to occur [58].

Numerous studies have explored the implementation of machine learning algorithms for predictive analysis. The following examples are especially significant.

Goyal et al. discuss AI's role in analyzing large amounts of data from industrial environments to detect and prevent cyber threats, highlighting AI-based cybersecurity techniques, including predictive analytics [59]. Das et al. propose an AI-envisioned blockchain-enabled key management scheme for industrial cyber–physical systems, discussing how AI can enhance IAM by securing data and preventing unauthorized access [60]. Koursioumpas et al. introduce PRIMATE, an AI-driven framework for profiling the networking behavior of devices and users in industrial environments [61]. Alomari et al. provide a systematic analysis of AI-based platforms for identifying governance and access control in industrial environments [10]. Lepenioti et al. propose a prescriptive analytics approach using interactive multi-objective reinforcement learning (IMORL) for decision-making in complex environments, applying AI and predictive analytics to optimize IAM processes [62].

4.3. Adaptive Authentication Mechanisms

Adaptive authentication mechanisms dynamically adjust security measures based on contextual information, balancing security with user convenience and reducing the likelihood of unauthorized access while minimizing disruptions for legitimate users. ML enhances authentication mechanisms by adapting them based on contextual information such as the user's location, time of access, and specific tasks being performed. Adaptive authentication can dynamically adjust security measures, such as requiring additional verification steps when anomalous behavior is detected.

Various studies have focused on applying machine learning algorithms for adaptive authentication mechanisms. Among these, the following deserve special mention.

Abuhasel introduces a zero-trust network-based access control scheme (ZTN-ACS) leveraging deep learning to enhance access control in Industry 5.0, focusing on mitigating adversarial threats [63]. Zou et al. explore the challenges and solutions in integrating AI models into existing industrial control systems, highlighting the benefits of well-trained ML models for optimizing access control [64]. Ogrezeanu discusses privacy-preserving AI solutions and the need for explainable AI in industrial applications, addressing challenges of secure access control while maintaining data privacy [65]. Leander et al. propose a method for automatic policy generation based on engineering data, emphasizing fine-grained access control policies to mitigate emerging cybersecurity threats [66]. Goyal et al. focus on AI's role in enhancing adaptive access control in Smart Industry 4.0 applications [59].

4.4. User Behavior Analytics (UBA)

User behavior analytics (UBA) leverage ML to understand and analyze the behavior of users within an industrial network. By building detailed profiles of user activities, ML

models can identify unusual or risky behaviors that may indicate compromised accounts or insider threats. UBA can detect subtle changes in user behavior that static rule-based systems might overlook, providing a more nuanced approach to access management [67].

The research in this area has delved into using machine learning algorithms for user behavior analytics. The following studies are among the most significant.

Tian et al. investigate detecting insiders' anomalous behaviors to prevent urban big data leakage using deep learning algorithms such as LSTM and convolutional LSTM to calculate deviations from normal daily behaviors [68]. Al-Qurishi et al. propose a platform using user-generated content, social graph connections, and user profile activities to detect anomalous behaviors [69]. Reguera-Bakhache et al. present a methodology to analyze operator–machine interaction patterns in industrial environments, improving usability and user experience [70]. Moysen et al. propose a framework using ML algorithms to analyze mobile network data, detect anomalies, and forecast performance [71]. Mihailescu et al. introduce an approach using advanced analytics techniques and ML to analyze user actions, patterns, and anomalies to identify potential threats, enhancing cybersecurity in industrial environments [72].

5. Future Directions

In the previous sections we have discussed the main AI technologies used in identification and authentication processes in industrial IAM systems and the advanced capabilities that the AI brings to IAM systems. In this section, we stress our literature review to answer the third research question: What are the main challenges and future lines of research?

As a result of this review, we found that, although the future of AI in industrial IAM is promising, to further advance the field, researchers and practitioners should consider some important issues and challenges to optimize AI applications in IAM systems. Among them, from our literature review, the following are particularly relevant.

5.1. Explainable AI (XAI)

Explainable AI (XAI) aims to develop AI systems that can explain their decisions and actions to human users, enhancing trust and accountability in IAM [73]. As AI-driven IAM systems make increasingly complex decisions regarding access control, it becomes essential for these systems to provide clear, understandable justifications for their actions [74]. Transparent AI fosters greater user trust, as individuals can comprehend how and why access decisions are made. This accountability is particularly important in sensitive and high-stakes environments, ensuring that AI systems operate fairly and consistently while allowing for human oversight and intervention when necessary.

5.2. Federated Learning

Implementing federated learning approaches to train AI models across decentralized industrial environments addresses the critical need to enhance AI capabilities without compromising data privacy [75]. Federated learning allows AI models to be trained collaboratively on data distributed across multiple locations, such as different industrial sites, without requiring the data to be centralized. This method ensures that sensitive information remains local, significantly reducing the risk of data breaches and privacy violations. By leveraging federated learning, industries can benefit from the collective intelligence and improved accuracy of AI models while maintaining stringent data privacy and security standards [76].

5.3. AI and Edge Computing

Leveraging edge computing to process access control data locally is essential for reducing latency and enhancing the responsiveness of IAM systems in real-time [77]. Edge computing enables data processing to occur closer to the source of data generation, such as IoT devices or local servers, rather than relying on centralized cloud infrastructure. This proximity reduces the time needed to process and analyze access control data, allowing

IAM systems to make quicker, more efficient decisions. By improving the speed and responsiveness of access control mechanisms, edge computing ensures that security measures are promptly enforced, thereby enhancing the overall effectiveness of IAM systems in dynamic industrial environments [78].

5.4. Integration with Innovative Technologies

Integrating AI-based IAM systems with innovative technologies like blockchain is increasingly necessary for achieving decentralized and secure access management. Blockchain technology provides a robust, tamper-proof ledger for recording access transactions, ensuring transparency and immutability [79]. When combined with AI, which excels in analyzing patterns and making real-time decisions, this integration enhances the security and efficiency of IAM systems. The decentralized nature of blockchain mitigates the risks associated with centralized data storage, reducing the likelihood of single points of failure and unauthorized access. This synergy between AI and blockchain fortifies access control mechanisms, ensuring secure, transparent, and efficient management of identities across various industrial and organizational landscapes [80].

6. Discussion

In this review of the current state-of-the-art of AI technologies and their applications in industrial IAM, it has been pointed how AI technologies have significantly increased the identification and authentication possibilities of IAM systems in industrial environments. Biometric recognition, reinforced by deep learning algorithms, has become a cornerstone of modern IAM systems, offering enhanced accuracy, reliability, and versatility. These technologies are essential for maintaining security and efficiency in industrial environments, where environmental conditions can be unpredictable and harsh.

Furthermore, AI technologies have significantly enhanced IAM systems by introducing advanced capabilities such as anomaly detection and real-time monitoring, predictive analytics, adaptive authentication mechanisms, and user behavior analytics. These capabilities leverage machine learning algorithms to analyze vast amounts of data, detect patterns, and make informed decisions in real-time. In industrial environments, these capabilities are crucial for maintaining security, preventing unauthorized access, and optimizing operational efficiency.

All these new capabilities draw a scenario where the future of AI in industrial IAM systems is promising, with several emerging trends and technologies poised to transform the field. The integration of explainable AI, federated learning, edge computing, and blockchain technology will play a crucial role in advancing AI applications in IAM systems, ensuring robust security measures and reliable access control mechanisms.

As a high-level summary of the impact of AI in IAM systems, Figure 2 is provided by the authors as a hierarchical representation of AI identification techniques within AI-powered IAM systems, illustrating their layered contributions to achieving operational efficiency, security, and scalability. This diagram tries to express in a graphical manner how AI brings into play several techniques for identification and authentication subsystems and, in general, for an IAM system. In relation to identification and authentication, AI techniques improve the multi-factor integration and biometric performance of the existing systems, mainly through the use of deep learning. In a more general scenario, AI could improve scalability, operational efficiency, and promote an enhanced security system based on the exploitation of AI properties for managing complex and extensive systems with different analytics, adaptive behavior, real-time capabilities, and anomaly detection and diagnosis through the existing techniques.

At the same time and based on the reviewed literature, while AI offers numerous benefits, it also presents challenges that must be addressed to ensure the effectiveness and security of IAM systems.

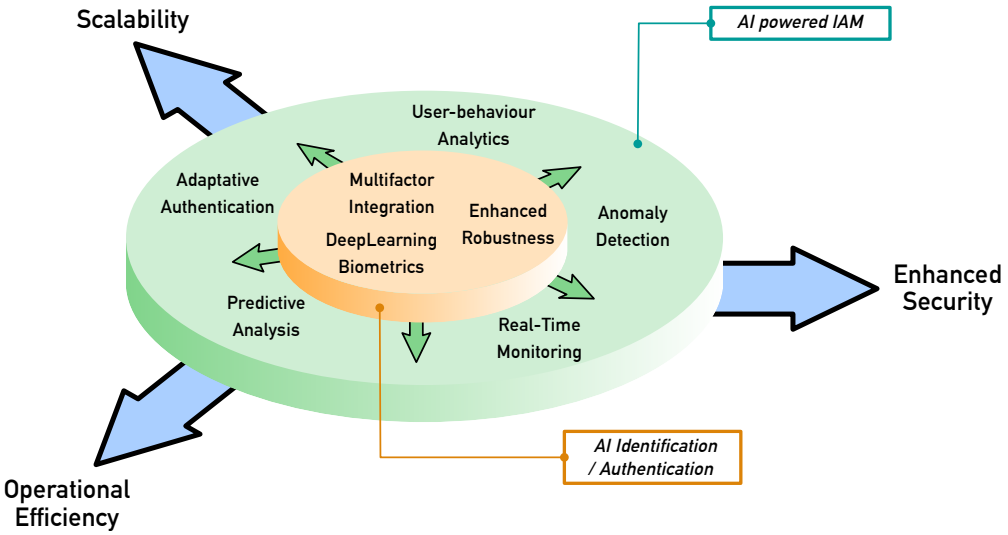

Figure 2. Main topics in AI-based IAM systems arranged from core techniques and challenges to main concerns and goals as stated in this survey by the authors. (Figure developed by the authors.)

6.1. Benefits of AI in IAM Systems

AI applications in IAM systems offer numerous benefits in terms of security, efficiency, and scalability, which are discussed below.

6.1.1. Enhanced Security

AI improves the accuracy and reliability of authentication and access control, reducing the likelihood of unauthorized access and security breaches [10]. By employing advanced algorithms and machine learning techniques, AI can analyze vast amounts of data to identify patterns and anomalies that might indicate a security threat. AI-powered systems continuously learn from new data, improving their ability to detect and prevent unauthorized access over time. These systems can adapt to evolving threats, providing robust security measures that are more resilient than traditional methods. Additionally, AI enables the implementation of multi-factor authentication and biometric recognition, further strengthening access control mechanisms and ensuring that only authorized individuals gain access to sensitive information [81].

6.1.2. Operational Efficiency

Automated and adaptive IAM systems reduce the need for manual oversight, allowing for more efficient management of access control in large and complex industrial environments [82]. These systems leverage automation to streamline user authentication, authorization, and auditing processes, ensuring that access permissions are consistently enforced without constant human intervention. Adaptive IAM systems dynamically adjust access controls based on real-time analysis of user behavior and context, providing a responsive and flexible security framework. This reduces the administrative burden, enhances operational efficiency, and allows security personnel to focus on more strategic tasks, ultimately leading to more robust and scalable access management in industrial settings.

6.1.3. Scalability

AI-driven IAM systems can scale to accommodate the growing number of devices and users in industrial settings, especially with the proliferation of IoT devices [83]. These advanced systems utilize AI to automate and optimize the management of identities and access permissions, ensuring that each device and user is accurately authenticated and authorized. As the number of IoT devices and connected users increases, AI-driven IAM systems can dynamically adjust and scale their operations to maintain robust security without compromising efficiency. By continuously learning from new data and adapting to

changes, these systems offer a resilient and scalable solution to manage the complex and expanding ecosystem of industrial IoT.

6.2. Challenges of AI in IAM Systems

However, while the adoption of AI in IAM systems offers numerous benefits, it also presents challenges that must be addressed to ensure the effectiveness and security of these systems. Among these challenges are data privacy, false positives/negatives, and implementation complexity.

6.2.1. Data Privacy

In AI-driven IAM systems, the extensive use of biometric data and user behavior analytics significantly enhances security but also raises substantial concerns regarding privacy and data protection [84]. These systems often rely on sensitive personal information, such as fingerprints, facial recognition, and behavioral patterns, to verify identities and monitor access. While these methods improve accuracy and reduce the risk of unauthorized access, they also pose potential risks if the data are mishandled or breached. Ensuring robust data protection measures and compliance with privacy regulations is critical to addressing these concerns and maintaining user trust in AI-driven IAM solutions.

6.2.2. False Positives/Negatives

AI-driven IAM systems, while highly advanced, are not immune to errors such as false positives and false negatives [85]. A false positive occurs when the system incorrectly identifies an authorized user or device as a threat, potentially causing unnecessary disruptions and access denials. Conversely, a false negative happens when the system fails to recognize an actual security threat, allowing unauthorized access. These errors can have significant implications, including reduced operational efficiency, compromised security, and decreased user trust. Addressing these challenges involves continuous system training, incorporating diverse data sets, and refining algorithms to improve accuracy and reliability in identity verification and access control.

6.2.3. Implementation Complexity

Integrating AI into existing IAM systems is a complex endeavor that demands significant investment in both technology and expertise [86]. This integration involves upgrading infrastructure, implementing advanced algorithms, and ensuring compatibility with current systems. It also requires specialized knowledge to effectively deploy and manage AI-driven solutions. The transition can be resource-intensive, necessitating substantial financial outlays and skilled personnel to handle the sophisticated technology. Despite these challenges, the long-term benefits of enhanced security, improved efficiency, and scalable access management make the investment worthwhile for organizations aiming to bolster their IAM capabilities. Organizations must carefully plan and execute these integrations to avoid disruptions.

6.3. Gaps and Proposed Directions

This review highlights promising opportunities to bridge the gaps in AI-driven IAM systems by addressing interoperability, scalability, ethical concerns and privacy. Below, we propose directions to advance the field.

One major issue is the lack of interoperability and standardized protocols across industries. This gap is particularly evident in environments where diverse legacy systems coexist with modern AI-driven frameworks, complicating seamless integration. The development of harmonized standards and APIs could address these inconsistencies, fostering smoother communication and compatibility between systems.

Another issue is the scalability of AI solutions within resource-constrained industrial settings. Legacy systems often lack the computational capacity to support sophisticated AI algorithms, posing barriers to widespread adoption. Exploring lightweight and adaptive AI

models optimized for edge devices could offer a practical solution, enabling the deployment of high-performing IAM systems without overburdening existing infrastructures.

Moreover, the reliance on AI for decision-making in IAM introduces ethical concerns, particularly around algorithmic biases. Decisions informed by biased datasets could lead to discriminatory practices, undermining trust in such systems. Incorporating fairness-aware machine learning techniques and regular audits of system decisions are crucial steps toward mitigating these risks. At the same time, the absence of benchmarking datasets and evaluation frameworks tailored to industrial IAM applications remains a significant limitation in the field. Establishing open-source resources would encourage consistent and replicable research efforts, paving the way for more robust and transparent advancements.

Privacy concerns also play a pivotal role in shaping the future of AI in IAM. Federated learning offers a promising approach by enabling organizations to collaboratively train models without compromising sensitive data. Such techniques not only enhance security but also address the increasing demand for privacy-preserving solutions in industrial environments.

Looking ahead, the field would benefit from research focused on dynamic policy adjustment mechanisms that leverage real-time user behavior analytics to fine-tune access control measures. Additionally, the creation of open-access datasets and privacy-preserving frameworks could further support the adoption and refinement of AI-based IAM systems. Together, these efforts could address the current gaps and catalyze the development of more effective and trustworthy solutions for industrial applications.

7. Conclusions

AI has revolutionized IAM in industrial environments by providing advanced, adaptive, and intelligent solutions to enhance security and operational efficiency.

For example, the integration of AI into IAM systems is set to significantly enhance security and operational efficiency within healthcare organizations. As healthcare continues its digital transformation, the protection of sensitive patient data has become a critical concern. AI-driven IAM solutions are particularly valuable in this context, as they help manage access control, ensure compliance with privacy regulations, and mitigate the risk of unauthorized access to medical records [87]. By leveraging machine learning, biometrics, and adaptive authentication methods, these systems can offer more secure, scalable, and efficient solutions compared to traditional IAM systems.

While challenges remain, ongoing advancements in AI technologies and methodologies continue to drive the evolution of IAM systems, ensuring they can meet the growing security demands of modern industrial operations.

In this paper, we have presented a comprehensive review of the current state-of-the-art AI technologies and their applications in industrial IAM systems conducted around three research questions.

In response to the first RQ "What are the main contributions of AI in identification and authentication with application in industrial IAM systems?", the study concludes that AI has significantly advanced the identification and authentication capabilities of IAM systems through biometric recognition comprising facial and voice recognition, whose accuracy, reliability, and versatility have been improved by deep learning algorithms. These technologies improve the accuracy, reliability, and versatility of IAM systems in industrial environments.

Next, after addressing the second RQ "What are the advanced capabilities that AI can bring to IAM systems?", the study shows that the most prominent advanced capabilities of AI-based IAM systems are real-time monitoring and anomaly detection, predictive analytics, adaptive authentication mechanisms, and user behavior analysis. These capabilities improve security, operational efficiency, and scalability in industrial environments, providing a more robust and adaptable IAM framework.

Finally, as a result of the third RQ "What are the main challenges and future lines of research?", the study allows us to conclude that the challenges and solutions in implement-

ing AI-based IAM systems include the integration of explainable AI, federated learning, edge computing, and blockchain technology. These emerging trends and technologies are poised to transform the field of IAM, enhancing security, efficiency, and scalability in industrial environments.

In conclusion, based on the reviewed literature, AI has significantly advanced IAM systems in industrial environments, providing sophisticated tools for security and efficiency. The continuous evolution of AI technologies promises to further enhance IAM capabilities, addressing current challenges and meeting future security needs.

Author Contributions: All authors contributed in all stages of the research and manuscript preparation. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare that they have no conflicts of interest.

Appendix A. Summary of Reviewed Articles

Table A1. Summary of the application domain, objective, methodology, and strengths of the articles considered in this review.

Application Domain	Subdomain	Reference	Objective	Methodology	Strengths
Access Control	ABAC	[14]	Protect PLCs with ABAC	Attribute-based access control model	Increased resilience against attacks
	Cloud	[22]	Secure access control in Azure environments	Design of secure access control solutions using Azure AD	Comprehensive guidelines for Azure security
	Context Modeling	[17]	Model context for access control	Context modeling for access control systems	Improved context-aware access control
	Industrial	[13]	Role- and node-based access control	Access control model for industrial networks	Enhanced security for industrial control systems
	RBAC	[12]	Decentralized role-centric authentication	Blockchain-enabled RC-AAM	Improved security and scalability
	TBAC	[16]	Develop task–role-based access control model	Integration of role-based and activity-based access control	Enhanced security and efficiency in enterprise environments
	User Identification	[41]	User identification using doorknob sensors	Deep learning algorithms on sensor data	High accuracy and feasibility for access control
AI	5G Networks	[61]	Context-aware profiling for 5G	AI-driven profiling techniques	Improved network management and security
	Applications	[1]	Increase resource efficiency	Systematic review of AI applications	Identifies AI's impact on resource efficiency
	Blockchain	[79]	Review blockchain for AI	Literature review	Identifies research challenges
	Cybersecurity	[52]	Malicious login detection	Graph neural network for login detection	Enhanced detection accuracy with GNN
		[76]	Analyze privacy attacks in federated learning	GAN-based attack framework	Effective user-level privacy attack
	Edge Computing	[77]	Ensure latency and reliability in edge computing	Distributed edge decision-making	Low-latency and reliable edge services
	Explainable	[73]	Explain AI systems to end users	Systematic literature review	Guidelines for AI system communication
	Governance and Access Control	[10]	AI-based governance and access control	Systematic analysis of AI platforms	Enhanced governance and access control
	Industrial Applications	[7]	Review industrial AI applications	Systematic review and framework proposal	Identifies challenges and opportunities in AI adoption
	Industrial Settings	[64]	Validate ML models in industrial settings	Framework for ML validation	Ensures reliability and accuracy of ML models

Table A1. *Cont.*

Application Domain	Subdomain	Reference	Objective	Methodology	Strengths
AI	Integration	[86]	Integration of AI systems	Proposal of integration methodologies	Solutions for building integrated AI systems
	LSTM	[55]	Robust anomaly detection in time series	Quantile LSTM with new activation function	High precision and recall in anomaly detection
	Privacy	[75]	Enhance privacy in federated learning	Privacy-enhanced federated learning scheme	Improved privacy and efficiency
	Privacy and Explainability	[65]	Ensure privacy and explainability in AI	Techniques for privacy and explainability	Balances performance with privacy concerns
	Quality Control	[37]	Quality control using deep learning	Deep learning on low-cost smart cameras	Cost-effective and accurate quality control
	Reinforcement Learning	[62]	Enhance decision-making with human-augmented analytics	Interactive multi-objective reinforcement learning	Improved decision making with human input
	Risks	[58]	Predict network security threats	Machine learning algorithms for threat prediction	Effective prediction of network threats
	Security	[8]	Enhance immigration and border control	AI-driven tools and predictive analytics	Improved security and operational efficiency
		[60]	Key management in industrial systems	Blockchain-enabled signature-based scheme	Secure and efficient key management
		[50]	AI for infrastructure protection	AI algorithms for threat detection and resilience	Advanced AI for real-time monitoring and response
	Trends	[5]	Apply AI in supply chain management	Systematic review and bibliometric analysis	Identifies AI trends and future research directions
Anomaly Detection	Big Data	[71]	Detect anomalies and forecast performance	Big-data-driven analysis	Accurate anomaly detection and forecasting
	Cloud	[85]	Reduce false positives in anomaly detection	Comparative analysis of AI techniques	Enhanced anomaly detection with reduced false positives
		[56]	Unsupervised anomaly detection	Time series clustering with KDetect algorithm	High accuracy and fast execution
	Cybersecurity	[51]	Abnormal login detection	Multi-source log fusion analysis	Effective detection of abnormal logins
	ICS Networks	[54]	Detect anomalies in ICS networks	Evolving decision trees using genetic programming	High accuracy in detecting network anomalies
	Security	[57]	Anomaly intrusion detection	Hybrid clustering–PSO algorithm	Optimized detection results with PSO
Biometrics	Deep Learning	[35]	Evaluate deep learning on serial fusion	Serial fusion of fingerprint, palm, and face using deep learning	Improved accuracy and user convenience
		[36]	Survey on deep learning for biometrics	Review of deep learning models for various biometrics	Extensive coverage of datasets and methods
		[28]	Survey on deep learning for biometrics	Review of deep learning techniques	Comprehensive survey of state-of-the-art methods
	Ethics	[84]	Ethical analysis of facial recognition	Examination of legal and ethical issues	Balances security with privacy concerns
	Face Recognition	[30]	Improve face recognition in low-quality images	Adaptive sparse representations	Effective in low-quality image scenarios
		[34]	Survey on deep face recognition	Review of deep learning techniques for face recognition	Comprehensive overview of methods and challenges
	Fingerprint	[46]	Review ML techniques for fingerprint recognition	Analysis of ML methods for fingerprint systems	Directions for future ML applications
		[47]	Detect fingerprint liveness	Deep residual network with adaptive learning	Improved liveness detection accuracy
	Industrial	[33]	Biometric authentication for industrial applications	Speaker recognition system	Robust authentication in industrial settings
	Iris Recognition	[48]	Survey on deep learning for iris recognition	Review of DL techniques for segmentation and recognition	Comprehensive analysis of DL applications
	Machine Learning	[29]	Advance biosensors with machine learning	Application of ML in biosensors	Enhanced sensor performance with ML

Table A1. *Cont.*

Application Domain	Subdomain	Reference	Objective	Methodology	Strengths
Biometrics	Multimodal	[31]	Develop a multimodal biometric system	Fusion of iris, face, and finger vein traits using CNNs	High accuracy with multimodal fusion
		[45]	Information fusion in biometrics	Fusion methodologies for multiple biometric traits	Enhanced performance over unimodal systems
	Obstacles	[44]	Address issues in biometric systems	Feature extraction methods for iris and fingerprint	Solutions for noisy artifacts and occlusions
	Recognition	[27]	Overview of biometric recognition	Analysis of biometric traits	High accuracy in identification
	Security	[38]	Compare biometric security systems	Deep structured learning for single, two, and three-mode systems	Performance comparison of different modes
		[42]	Overview of biometric security	Analysis of biometric technologies	Early insights into biometric security
	User Identification	[39]	Continuous authentication using behavioral biometrics	AI-driven analysis of behavioral signals	Improved security and user identification in IoT
		[40]	Identify users via door handle interaction	Sensor data analysis with dynamic time warping	High accuracy in user identification
	Voice Recognition	[32]	Review voice recognition technology	Analysis of current state and applications	Insights into industrial applications
IAM	Authentication	[82]	Review intelligent authentication for IAM	Evaluation of intelligent authentication key factors	Comprehensive review of IAM authentication methods
	Cloud	[21]	Address IAM mechanisms and challenges	Review of IAM mechanisms in cloud	Comprehensive analysis of IAM challenges
		[18]	Robust IAM for cloud systems	IAM framework with enhanced assurance	Improved security and continuous monitoring
		[19]	Generate interpretable security policies	Constraint programming and graph learning	Reduced security risks and improved policy management
	Enterprise	[25]	Extend IAM architecture with dynamic information	Integration of additional information sources	Enhanced IAM processes with real-time data
	Federated Environments	[24]	Evaluate IAM system performance	System model and metrics for performance evaluation	Quantitative measures for IAM system architectures
	Healthcare	[26]	Secure electronic healthcare records	IAM systems for healthcare data protection	Improved data security and operational efficiency
		[87]	Future of IAM in healthcare	Analysis of AI in IAM for healthcare	Improved IAM with AI integration
	Machine Learning	[49]	Survey on ML in IAM systems	Deep dive into ML applications in IAM	Insights into ML-driven IAM enhancements
	Management	[23]	Improve IAM data quality	TAQM approach for measuring and improving IAM data quality	Structured process for attribute quality management
	Market	[9]	Analyze IAM market trends	Market size, share, and forecast analysis	Insights into market growth and trends
	Networking	[20]	Enforce MLS policies in unstable networks	SDN controller application	Efficient and adaptive security policy enforcement
	Security	[2]	Highlight IAM importance in security systems	Framework of processes, policies, and technologies	Centralized user management and authentication
Industrial	Automation	[6]	Safe human–robot collaboration	Mixed-perception approach	Enhanced safety with visual and tactile perception
	HMI	[70]	Adapt HMI based on interaction	Sequence similarity analysis	Improved operator–machine interaction
	Sensors	[43]	Precision in harsh environments	Multidisciplinary approach for sensor and actuator systems	High reliability and autonomy in harsh conditions
Industry 4.0	Access Control	[63]	Implement zero-trust access control	Deep learning for access control	Enhanced security and resilience
		[66]	Develop ideal access control strategy	Evaluation of access control strategies	Improved security for manufacturing systems
		[15]	PLM with multigranularity access control	Multigranularity access control model	Optimized product life cycle management
	Cybersecurity	[59]	Integrate AI with cybersecurity	AI-driven solutions for smart industry	Enhanced security for Industry 4.0 applications

Table A1. *Cont.*

Application Domain	Subdomain	Reference	Objective	Methodology	Strengths
IoT	AI	[81]	Enhance IoT security with AI	AI-driven authentication and authorization	Fast and secure IoT authentication
	Blockchain	[80]	Blockchain-based IAM for IoT	Private blockchain for IAM	Tamper-proof and scalable IAM
	Cybersecurity	[3]	Detect cybersecurity attacks	Systematic literature review of AI methods	Comprehensive analysis of AI techniques
	General	[78]	Optimize task offloading in IoT	Logic-based benders decomposition	Efficient task scheduling and resource allocation
	Identity Authentication	[11]	Research centralized identity authentication	Management application platform	Enhanced security and management efficiency
	Industrial	[83]	Review AI models in IIoT	Analysis of AI models and tools for IIoT	Holistic overview of AI-enabled IIoT systems
	Risk	[4]	Develop smart helmet for safety	AI-driven platform for risk detection	Real-time monitoring and risk evaluation
User Behavior	Analysis	[69]	Identify malicious activities	Analysis of user behavior	Detects malicious activities in large-scale networks
	Anomaly Detection	[53]	Anomaly detection of user behaviors	Machine learning-based detection method	Effective in identifying user behavior anomalies
	Cybersecurity	[72]	Enhance cybersecurity using user behavior analysis	Analysis of user behavior patterns	Improved threat detection
	Healthcare	[74]	Persuasive explainable AI for behavior change	Natural language generation	Effective in reducing unhealthy behaviors
	Intrusion Detection	[67]	Detect host-based intrusions	Dynamic and static behavioral models	Effective anomaly detection
	Machine Learning	[68]	Analyze user and entity behavior	Machine learning-based detection	Effective in identifying anomalies

References

1. Waltersmann, L.; Kiemel, S.; Stuhlsatz, J.; Sauer, A.; Miehe, R. Artificial Intelligence Applications for Increasing Resource Efficiency in Manufacturing Companies—A Comprehensive Review. *Sustainability* **2021**, *13*, 6689. [CrossRef]
2. Singh, C.; Thakkar, R.G.; Warraich, J. IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. *Eur. J. Eng. Technol. Res.* **2023**, *8*, 30–38. [CrossRef]
3. Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics* **2022**, *11*, 198. [CrossRef]
4. Campero-Jurado, I.; Sánchez, S.M.; Gomez, J.; Rodríguez, S.; Corchado, J. Smart Helmet 5.0 for Industrial Internet of Things Using Artificial Intelligence. *Sensors* **2020**, *20*, 6241. [CrossRef] [PubMed]
5. Pournader, M.; Ghaderi, H.; Hassanzadegan, A.; Fahimnia, B. Artificial intelligence applications in supply chain management. *Int. J. Prod. Econ.* **2021**, *241*, 108250. [CrossRef]
6. Amin, F.M.; Rezayati, M.; Venn, H.W.V.D.; Karimpour, H. A Mixed-Perception Approach for Safe Human-Robot Collaboration in Industrial Automation. *Sensors* **2020**, *20*, 6347. [CrossRef] [PubMed]
7. Peres, R.S.; Jia, X.; Lee, J.; Sun, K.; Colombo, A.; Barata, J. Industrial Artificial Intelligence in Industry 4.0 - Systematic Review, Challenges and Outlook. *IEEE Access* **2020**, *8*, 220121–220139. [CrossRef]
8. Alam, M.N.; Kabir, M.S.; Sumi, E.J. Artificial Intelligence (AI) and Future Immigration and Border Control. *Int. J. Multidiscip. Res.* **2023**, *5*, 1–7. [CrossRef]
9. Grand View Research. Identity and Access Management Market Size, Share & Trends Analysis Report by End-Use (BFSI, Education), by Component (Directory Service, Provisioning), by Deployment (Cloud, on-Premise), and Segment Forecasts, 2023–2030. 2024. Available online: https://www.grandviewresearch.com/industry-analysis/identity-access-management-iam-market (accessed on 14 November 2024).
10. Alomari, M.; Khan, H.U.; Khan, S.; Al-Maadid, A.; Abu-Shawish, Z.K.; Hammami, H. Systematic Analysis of Artificial Intelligence-Based Platforms for Identifying Governance and Access Control. *Secur. Commun. Netw.* **2021**, *2021*, 8686469. [CrossRef]
11. Fang, J.; Yan, C.; Yan, C. Centralized identity authentication research based on management application platform. In Proceedings of the 2009 First International Conference on Information Science and Engineering, IEEE, Washington, DC, USA, 26–28 December 2009; pp. 2292–2295. [CrossRef]
12. Rashid, A.; Masood, A.; Khan, A.u.R. RC-AAM: Blockchain-enabled decentralized role-centric authentication and access management for distributed organizations. *Clust. Comput.* **2021**, *24*, 3551–3571. [CrossRef]

13. Wang, S.; Yang, Y.; Xia, T.; Zhang, W. A role and node based access control model for industrial control network. In Proceedings of the 2nd International Conference on Cryptography, Security and Privacy, Guiyang, China, 16–19 March 2018; pp. 89–94. [CrossRef]
14. Gowdanakatte, S.; Ray, I.; Hilde Houmb, S. Attribute based access control model for protecting programmable logic controllers. In Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, Washington, DC, USA, 27 April 2022; pp. 47–56. [CrossRef]
15. Yu, L.; Zhu, S. Industry 4.0 Engineering Product Life Cycle Management Based on Multigranularity Access Control Model. *Comput. Intell. Neurosci.* **2022**, *2022*, 3655621. [CrossRef] [PubMed]
16. Oh, S.; Park, S. Task–role-based access control model. *Inf. Syst.* **2003**, *28*, 533–562. [CrossRef]
17. Sladić, G.; Milosavljević, B.; Konjović, Z. Modeling context for access control systems. In Proceedings of the 2012 IEEE 10th Jubilee International Symposium on Intelligent Systems and Informatics, IEEE, Subotica, Serbia, 20–22 September 2012; pp. 37–42. [CrossRef]
18. Johnson, F.M.P.D. *Robust Identity and Access Management for Cloud Systems*; Concordia University of Edmonton: Edmonton, AB, Canada, 2020. [CrossRef]
19. Kazdagli, M.; Tiwari, M.; Kumar, A. Using constraint programming and graph representation learning for generating interpretable cloud security policies. *arXiv* **2022**. [CrossRef]
20. Burke, Q.; Mehmeti, F.; George, R.; Ostrowski, K.; Jaeger, T.; La Porta, T.F.; McDaniel, P. Enforcing multilevel security policies in unstable networks. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 2349–2365. [CrossRef]
21. Indu, I.; Anand, P.R.; Bhaskar, V. Identity and access management in cloud environment: Mechanisms and challenges. *Eng. Sci. Technol. Int. J.* **2018**, *21*, 574–588. [CrossRef]
22. Ots, K. Identity and Access Management. In *Azure Security Handbook: A Comprehensive Guide for Defending Your Enterprise Environment*; Apress: Berkeley, CA, USA, 2021; pp. 11–38. [CrossRef]
23. Kunz, M.; Puchta, A.; Groll, S.; Fuchs, L.; Pernul, G. Attribute quality management for dynamic identity and access management. *J. Inf. Secur. Appl.* **2019**, *44*, 64–79. [CrossRef]
24. Schell, F.; Dinger, J.; Hartenstein, H. Performance evaluation of identity and access management systems in federated environments. In *Proceedings of the Scalable Information Systems: 4th International ICST Conference, INFOSCALE 2009, Hong Kong, 10–11 June 2009*; Revised Selected Papers 4; Springer: Berlin/Heidelberg, Germany, 2009; pp. 90–107. [CrossRef]
25. Puchta, A.; Groll, S.; Pernul, G. Leveraging Dynamic Information for Identity and Access Management: An Extension of Current Enterprise IAM Architecture. In Proceedings of the ICISSP, Virtual, 11–13 February 2021; pp. 611–618. [CrossRef]
26. Anand, D.; Khemchandani, V. Identity and access management systems. In *Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms and Solutions*; IET—Institution of Engineering and Technology: London, UK, 2019; p. 61. [CrossRef]
27. Jain, A.K.; Kumar, A. Biometric recognition: An overview. In *Second Generation Biometrics: The Ethical, Legal and Social Context*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 49–79. [CrossRef]
28. Sundararajan, K.; Woodard, D. Deep Learning for Biometrics: A survey. *ACM Comput. Surv. (CSUR)* **2018**, *51*, 1–34. [CrossRef]
29. Cui, F.; Yue, Y.; Zhang, Y.; Zhang, Z.; Zhou, H.S. Advancing Biosensors with Machine Learning. *ACS Sensors* **2020**, *5*, 3346–3364. [CrossRef] [PubMed]
30. Heinsohn, D.; Villalobos, E.; Prieto, L.; Mery, D. Face recognition in low-quality images using adaptive sparse representations. *Image Vis. Comput.* **2019**, *85*, 46–58. [CrossRef]
31. Alay, N.; Al-Baity, H.H. Deep Learning Approach for Multimodal Biometric Recognition System Based on Fusion of Iris, Face, and Finger Vein Traits. *Sensors* **2020**, *20*, 5523. [CrossRef]
32. Fegade, S.V.; Chaturvedi, A.; Agarwal, M. Voice Recognition Technology: A Review. *Int. J. Adv. Res. Sci. Commun. Technol.* **2021**, *8*, 31–34. [CrossRef]
33. Shayamunda, C.; Ramotsoela, T.; Hancke, G.P. Biometric authentication system for industrial applications using speaker recognition. In Proceedings of the IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society, IEEE, Singapore, 18–21 October 2020; pp. 4459–4464. [CrossRef]
34. Wang, M.; Deng, W. Deep face recognition: A survey. *Neurocomputing* **2021**, *429*, 215–244. [CrossRef]
35. Edwards, T.; Hossain, M.S. Effectiveness of deep learning on serial fusion based biometric systems. *IEEE Trans. Artif. Intell.* **2021**, *2*, 28–41. [CrossRef]
36. Minaee, S.; Abdolrashidi, A.; Su, H.; Bennamoun, M.; Zhang, D. Biometrics recognition using deep learning: A survey. *Artif. Intell. Rev.* **2023**, *56*, 8647–8695. [CrossRef]
37. Toigo, S.; Cenedese, A.; Fornasier, D.; Kasi, B. Deep-learning based industrial quality control on low-cost smart cameras. In *Proceedings of the Sixteenth International Conference on Quality Control by Artificial Vision, Albi, France, 6–8 June 2023*; International Society for Optics and Photonics: Bellingham, WA, USA, 2023; Volume 12749, pp. 108–116. [CrossRef]
38. Atanda, O.G.; Abiodun, M.K.; Awotunde, J.B.; Adeniyi, J.K.; Adeniyi, A.E. A Comparative Study of the Performances of Single-mode, Two-mode, and Three-mode Biometric Security Systems Using Deep Structured Learning Technique. In Proceedings of the 2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG), IEEE, Omu-Aran, Nigeria, 5–7 April 2023; Volume 1, pp. 1–10. [CrossRef]
39. Liang, Y.; Samtani, S.; Guo, B.; Yu, Z. Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. *IEEE Internet Things J.* **2020**, *7*, 9128–9143. [CrossRef]

40. Vegas, J.; Llamas, C.; González, M.A.; Hernández, C. Identifying users from the interaction with a door handle. *Pervasive Mob. Comput.* **2021**, *70*, 101293. [CrossRef]
41. Vegas, J.; Rao, A.R.; Llamas, C. Deep Learning System for User Identification Using Sensors on Doorknobs. *Sensors* **2024**, *24*, 5072. [CrossRef] [PubMed]
42. Lawton, G. Biometrics: A new era in security. *Computer* **1998**, *31*, 16–18. [CrossRef]
43. French, P.; Krijnen, G.; Roozeboom, F. Precision in harsh environments. *Microsyst. Nanoeng.* **2016**, *2*, 1–12. [CrossRef] [PubMed]
44. Gawande, U.; Golhar, Y.; Hajari, K. Biometric-Based Security System: Issues and Challenges. In *Intelligent Techniques in Signal Processing for Multimedia Security*; Springer International Publishing: Cham, Switzerland, 2017; pp. 151–176. [CrossRef]
45. Ross, A.A.; Jain, A.K.; Nandakumar, K. Information fusion in biometrics. In *Handbook of Multibiometrics*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 37–58.
46. Yadav, J.; Jaffery, Z.A.; Singh, L. A short review on machine learning techniques used for fingerprint recognition. *J. Crit. Rev.* **2020**, *7*, 2768–2773. [CrossRef]
47. Yuan, C.; Xia, Z.; Sun, X.; Wu, Q.M.J. Deep Residual Network With Adaptive Learning Framework for Fingerprint Liveness Detection. *IEEE Trans. Cogn. Dev. Syst.* **2020**, *12*, 461–473. [CrossRef]
48. Nguyen, K.; Proença, H.; Alonso-Fernandez, F. Deep learning for iris recognition: A survey. *arXiv* **2022**, arXiv:2210.05866. [CrossRef]
49. Aboukadri, S.; Ouaddah, A.; Mezrioui, A. Machine Learning in Identity and Access Management Systems: Survey and Deep Dive. *Comput. Secur.* **2024**, *139*, 103729. [CrossRef]
50. Sarker, I.H. AI for Critical Infrastructure Protection and Resilience. In *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 153–172. [CrossRef]
51. Tao, J.; Wang, W.; Zheng, N.; Han, T.; Chang, Y.; Zhan, X. An Abnormal Login Detection Method Based on Multi-source Log Fusion Analysis. In Proceedings of the 2019 IEEE International Conference on Big Knowledge (ICBK), Beijing, China, 10–11 November 2019; pp. 229–235. [CrossRef]
52. Liu, F.; Wen, Y.; Wu, Y.; Liang, S.; Jiang, X.; Meng, D. MLTracer: Malicious Logins Detection System via Graph Neural Network. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December 2020; pp. 715–726. [CrossRef]
53. Tian, X.G.; Gao, L.Z.; Sun, C.L.; Duan, M.Y.; Zhang, E.Y. A Method for Anomaly Detection of User Behaviors Based on Machine Learning. *J. China Univ. Posts Telecommun.* **2006**, *13*, 61–78. [CrossRef]
54. Hosic, J.; Lamps, J.; Hart, D.H. Evolving decision trees to detect anomalies in recurrent ICS networks. In Proceedings of the 2015 World Congress on Industrial Control Systems Security (WCICSS), IEEE, London, UK, 14–16 December 2015; pp. 50–57. [CrossRef]
55. Saha, S.; Sarkar, J.; Dhavala, S.; Mota, P.; Sarkar, S. quantile-Long Short Term Memory: A Robust, Time Series Anomaly Detection Method. *IEEE Trans. Artif. Intell.* **2024**, *5*, 3939–3950. [CrossRef]
56. Sharma, S.; Diarra, A.; Alvares, F.; Ropars, T. KDetect: Unsupervised Anomaly Detection for Cloud Systems Based on Time Series Clustering. In Proceedings of the 3rd International Workshop on Systems and Network Telemetry and Analytics, New York, NY, USA, 23 June 2020; pp. 3–10. [CrossRef]
57. Zheng, H.; Hou, M.; Wang, Y. An Efficient Hybrid Clustering-PSO Algorithm for Anomaly Intrusion Detection. *J. Softw.* **2011**, *6*, 2350–2360. [CrossRef]
58. Nitesh, K.T.; Thirumala, A.K.; Mohammed, U.F.; Ahmed, M.R. Network Security Threat Detection: Leveraging Machine Learning Algorithms for Effective Prediction. In Proceedings of the 12th International Conference on Advanced Computing (ICoAC), IEEE, Chennai, India, 17–19 August 2023; pp. 1–5. [CrossRef]
59. Goyal, S.; Rajawat, A.S.; Solanki, R.K.; Zaaba, M.A.M.; Long, Z.A. Integrating AI with cyber security for smart industry 4.0 application. In Proceedings of the 2023 International Conference on Inventive Computation Technologies (ICICT), IEEE, Lalitpur, Nepal, 26–28 April 2023; pp. 1223–1232. [CrossRef]
60. Das, A.K.; Bera, B.; Saha, S.; Kumar, N.; You, I.; Chao, H.C. AI-envisioned blockchain-enabled signature-based key management scheme for industrial cyber–physical systems. *IEEE Internet Things J.* **2022**, *9*, 6374–6388. [CrossRef]
61. Koursioumpas, N.; Barmpounakis, S.; Stavrakakis, I.; Alonistioti, N. AI-driven, Context-Aware Profiling for 5G and Beyond Networks. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 1036–1048. [CrossRef]
62. Lepenioti, K.; Bousdekis, A.; Apostolou, D.; Mentzas, G. Human-augmented prescriptive analytics with interactive multi-objective reinforcement learning. *IEEE Access* **2021**, *9*, 100677–100693. [CrossRef]
63. Abuhasel, K.A. A Zero-Trust Network-Based Access Control Scheme for Sustainable and Resilient Industry 5.0. *IEEE Access* **2023**, *11*, 116398–116409. [CrossRef]
64. Zou, H.; Chen, G.; Xie, P.; Chen, S.; He, Y.; Huang, H.; Nie, Z.; Zhang, H.; Bala, T.; Tulip, K.; et al. Validate and Enable Machine Learning in Industrial AI. *arXiv* **2020**. [CrossRef]
65. Ogrezeanu, I.; Vizitiu, A.; Ciusdel, C.; Puiu, A.; Coman, S.; Boldisor, C.; Itu, A.; Demeter, R.; Moldoveanu, F.; Suciu, C.; et al. Privacy-preserving and explainable AI in industrial applications. *Appl. Sci.* **2022**, *12*, 6395. [CrossRef]
66. Leander, B.; Čaušević, A.; Hansson, H.; Lindström, T. Toward an ideal access control strategy for industry 4.0 manufacturing systems. *IEEE Access* **2021**, *9*, 114037–114050. [CrossRef]

67. Yeung, D.; Ding, Y. Host-based intrusion detection using dynamic and static behavioral models. *Pattern Recognit.* **2003**, *36*, 229–243. [CrossRef]
68. Tian, Z.; Luo, C.; Lu, H.; Su, S.; Sun, Y.; Zhang, M. User and Entity Behavior Analysis under Urban Big Data. *ACM Trans. Data Sci.* **2020**, *1*, 1–19. [CrossRef]
69. Al-Qurishi, M.; Hossain, M.S.; Alrubaian, M.; Rahman, S.M.M.; Alamri, A. Leveraging analysis of user behavior to identify malicious activities in large-scale social networks. *IEEE Trans. Ind. Informatics* **2018**, *14*, 799–813. [CrossRef]
70. Reguera-Bakhache, D.; Garitano, I.; Uribeetxeberria, R.; Cernuda, C. An industrial hmi temporal adaptation based on operator-machine interaction sequence similarity. In Proceedings of the 2021 22nd IEEE International Conference on Industrial Technology (ICIT), IEEE, Virtual, 10–12 March 2021; Volume 1, pp. 1021–1026. [CrossRef]
71. Moysen, J.; Ahmed, F.; García-Lozano, M.; Niemelä, J. Big data-driven automated anomaly detection and performance forecasting in mobile networks. In Proceedings of the 2020 IEEE Globecom Workshops, GC Wkshps, IEEE, Taipei, Taiwan, 7–11 December 2020; pp. 1–5. [CrossRef]
72. Mihailescu, M.I.; Nita, S.L.; Rogobete, M.; Marascu, V. Unveiling Threats: Leveraging User Behavior Analysis for Enhanced Cybersecurity. In Proceedings of the 2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), IEEE, Bucharest, Romania, 29–30 June 2023; pp. 1–6. [CrossRef]
73. Laato, S.; Tiainen, M.; Islam, A.K.M.N.; Mäntymäki, M. How to explain AI systems to end users: A systematic literature review and research agenda. *Internet Res.* **2022**, *32*, 1–31. [CrossRef]
74. Dragoni, M.; Donadello, I.; Eccher, C. Explainable AI meets persuasiveness: Translating reasoning results into behavioral change advice. *Artif. Intell. Med.* **2020**, *105*, 101840. [CrossRef] [PubMed]
75. Hao, M.; Li, H.; Luo, X.; Xu, G.; Yang, H.; Liu, S. Efficient and Privacy-Enhanced Federated Learning for Industrial Artificial Intelligence. *IEEE Trans. Ind. Informatics* **2020**, *16*, 6532–6542. [CrossRef]
76. Song, M.; Wang, Z.; Zhang, Z.; Song, Y.; Wang, Q.; Ren, J.; Qi, H. Analyzing User-Level Privacy Attack Against Federated Learning. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 2430–2444. [CrossRef]
77. Elbamby, M.S.; Perfecto, C.; Liu, C.F.; Park, J.; Samarakoon, S.; Chen, X.; Bennis, M. Wireless Edge Computing With Latency and Reliability Guarantees. *Proc. IEEE* **2019**, *107*, 1717–1737. [CrossRef]
78. Alameddine, H.; Sharafeddine, S.; Sebbah, S.; Ayoubi, S.; Assi, C. Dynamic Task Offloading and Scheduling for Low-Latency IoT Services in Multi-Access Edge Computing. *IEEE J. Sel. Areas Commun.* **2019**, *37*, 668–682. [CrossRef]
79. Salah, K.; Rehman, M.H.; Nizamuddin, N.; Al-Fuqaha, A.I. Blockchain for AI: Review and Open Research Challenges. *IEEE Access* **2019**, *7*, 10127–10149. [CrossRef]
80. Nuss, M.; Puchta, A.; Kunz, M. Towards blockchain-based identity and access management for internet of things in enterprises. In *Proceedings of the Trust, Privacy and Security in Digital Business: 15th International Conference, TrustBus 2018, Regensburg, Germany, 5–6 September 2018*; Proceedings 15; Springer: Berlin/Heidelberg, Germany, 2018; pp. 167–181. [CrossRef]
81. Fang, H.; Qi, A.; Wang, X. Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement. *IEEE Netw.* **2019**, *34*, 24–29. [CrossRef]
82. Mohammed, I.A. Intelligent authentication for identity and access management: A review paper. *Int. J. Manag. IT Eng. (IJMIE)* **2013**, *3*, 696–705. [CrossRef]
83. Dini, P.; Diana, L.; Elhanashi, A.; Saponara, S. Overview of AI-Models and Tools in Embedded IIoT Applications. *Electronics* **2024**, *13*, 2322. [CrossRef]
84. Smith, M.; Miller, S. The ethical application of biometric facial recognition technology. *Ai Soc.* **2022**, *37*, 167–175. [CrossRef] [PubMed]
85. Olateju, O.O.; Okon, S.U.; Igwenagu, U.T.I.; Salami, A.A.; Oladoyinbo, T.O.; Olaniyi, O.O. Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud. *Asian J. Res. Comput. Sci.* **2024**, *17*, 264–292. [CrossRef]
86. Thórisson, K.R. Integrated AI systems. *Minds Mach.* **2007**, *17*, 11–25. [CrossRef]
87. Syed, F.M.; ES, F.K.; Johnson, E. AI and the Future of IAM in Healthcare Organizations. *Int. J. Adv. Eng. Technol. Innov.* **2022**, *1*, 363–392.