International Journal of Scientific Research and Engineering Development– Volume 9 Issue 4, July – August 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

A Survey of Artificial Intelligence Applications in Identity and Access Management (IAM)

Sharad Sharma
Artificial Intelligence
Sharadiitkanpur@gmail.com

----------**********----------

Abstract:

Identity and Access Management (IAM) is fundamental to organizational security strategy. Factors like increasing users and system complexity make access control administration increasingly difficult. Further managing access for different types of users like employees, future dated employees, contractors, vendors, suppliers, alumni make the access controls further complicated. Traditional IAM solutions often fail to address complex scenarios in today's organizations facing sophisticated security attacks. The evolution of work methods, including mobility, cloud computing, and collaborative platforms, requires adaptation of access control systems. Artificial Intelligence (AI) has revolutionized IAM through advanced techniques enabling instant and continuous authentication and access control, as this paper explores. The paper provides an IAM systems overview, examines AI tools for biometric authentication and dynamic access control based on existing literature, and analyzes privacy, security threats, ethics and laws. Finally, it presents a synthesis of existing works to contribute to understanding AI's application in access control, examining its benefits, threats, and future implications.

Keywords: Identity and Access Management (IAM); Artificial Intelligence (AI); Machine Learning; Biometric Authentication; Internet of Things (IoT); Attribute based access control(ABAC); Policy based access controls (PBAC); Identity Verification; Access Control; Cybersecurity; Privacy; Deep Learning; Segregation of Duties (SOD); Behavioral Biometrics; Algorithmic Bias; Regulatory Compliance

----------**********----------

1. Introduction

Identity and Access Management (IAM) is crucial in all the modern facets including but not limited to access management, continuous monitoring, application security, secure by design application development, security operations centers, modern computing. With interconnected technology, managing security and identity information protects organizations' systems and the individuals they interact with. Whether logging into networks, accessing online banking, or creating social media accounts, identity verification and access authorization forms the foundation of modern technological interactions. An Identity and Access Management (IAM) system comprises policies, technologies, and processes for managing identity and access to all organizational resources including computing resources. Most IAM solutions use traditional static, rule-based access control techniques including password authentication, role-based access control (RBAC) or Attribute based access control(ABAC) or Policy based access controls (PBAC), and predefined multi-factor authentication (MFA). However, these outdated approaches no longer suffice for today's digital realities. With cloud, IoT and mobile devices, remote workers both corporate and non-corporate and sophisticated attacks, the attack surface has increased, leaving legacy IAM solutions vulnerable to risks including

compromised credentials, insider threats and account takeover. Legacy IAM solutions impede business productivity by requiring excessive authentication and authorization time. Artificial Intelligence (AI), Machine Learning (ML) and Deep Learning (DL) can transform digital asset interaction. Current IAM solutions use static rules for authentication and authorization, becoming complex as users and systems grow, leading to poor user experiences - contradicting IAM's purpose. AI adoption in IAM can reduce this complexity and provide better security. Next generation AI, ML and DL-based solutions can replace static rules with behavior analysis to implement real-time access controls based on user behavior. The intersection of artificial intelligence (AI) and identity and access management (IAM) is transforming how IT organizations manage identity and access. This reflects a fundamental change in authentication and authorization processes. Historically, authentication was a one-time event where users logged into a Personal Computer (PC) with username and password to access resources. Now, with AI advancements, authentications are risk-based and real-time. Your login credentials are no longer just username and password with one-time authentication. These may be challenged more frequently during sessions, if access is granted. Systems will analyze multi-modal biometrics in real-time including voice, behavior and facial recognition to verify identity. Many routine IAM tasks will be automated through AI. While combining AI and identity management offers compelling benefits, it presents significant challenges. Key challenges include privacy, PII protection, algorithmic bias, end user experiences, cost to enable and manage and security of identification data. Systems using advanced authentication methods will likely become prime targets for attacks. Auditing and producing audit trail/evidence for these "black box" AI systems' decision-making will be challenging, as will ensuring non-discriminatory access controls (Basak et al., 2024; Mishra, 2024).

This paper surveys Artificial Intelligence (AI) in Identity and Access Management (IAM) based on recent research. Section 2 presents IAM systems and their building blocks. Section 3 describes AI's role in identity verification, and Section 4 covers AI techniques in biometric authentication. Section 5 presents AI techniques in dynamic access control models. Section 6 discusses privacy and security challenges in AI-enabled IAM systems. Section 7 addresses ethical and regulatory implications, while Section 8 presents final considerations and highlights promising research.

2. Overview of Identity Management Systems

Identity and Access Management (IAM) is about policies, technologies and processes that manage user identities and give users access to the applications, services and data they need to perform their work. IAM is about securing access to resources so that legitimate users have access to what they need to perform their job functions and at the same time preventing unauthorized access to resources that if compromised could potentially cause harm to an organization such as breach, data theft or compromise of sensitive data. IAM also enables access governances to manage access of users by enabling periodic review of user's access and also enabling Segregation of Duties (SOD). IAM is evolving from an administrative function in IT to a strategic role within security as a result of evolving trends such as the move to the cloud, digital transformations, IoT, mobile workers and the use of third-party integrations (Filho, 2025).

2.1 Core Components of IAM Systems

Traditional IAM architectures have five main components: Identity lifecycle management, Authentication Service, Authorization Service, Access Governance and Directory Services.

- **Identity Lifecycle Management:** Identity Lifecycle Management (ILM) involves creating, modifying and deleting digital identities through provisioning users with appropriate access and de-provisioning when functions change or users leave. ILM has both security and compliance roots.

- **Authentication:** Authentication validates user identity by requesting authentication factors: something the user knows, possesses, or has that can be measured. Most systems use basic single-factor authentication. Multi-factor authentication (MFA) requests multiple authentication factors from users. While MFA offers more security than passwords, it remains vulnerable to attacks like phishing and poses risks in Enterprise.
- **Authorization:** After authentication, Authorization determines what actions users can perform on a system. Two common models are Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). RBAC assigns users roles with allowed actions, while ABAC makes decisions based on user, resource, and environmental attributes. RBAC is common but not always sufficient.
- **Access Governance:** Periodic review of user's access by their manager or application owners or privileged role owner ensures that users have the right access on a periodic basis. Further enforcing both preventive and detective Segregation of Duties also enforce access governance.
- **Directory Services:** Directory Services is a database storing information about entities like individuals, groups, computers, or organizations. It contains user account information and passwords in a centralized database. A common type is the Lightweight Directory Access Protocol (LDAP) directory, with Microsoft Active Directory being the most common. More companies are migrating to cloud Directory Services rather than on premises servers.

These limitations on static analysis and material behavior will be highlighted in following subsections, demonstrating why this field requires the use of AI (Filho, 2025; Lesavre, 2020; Zhang et al., 2020).

2.2 IAM Architectures and Deployment Models

Identity and Access Management (IAM) architectures have evolved to meet business needs. On premises IAM is the legacy model where components are deployed in the business data center with IT maintaining complete control. These solutions require significant capital investment and extensive administration. Cloud IAM simplifies infrastructure and administrative workload, helping organizations adopt new cloud applications quickly. Hybrid IAM combines on premises and cloud-based solutions, allowing businesses to leverage legacy systems while gaining cloud capabilities. Identity Fabric is an architectural concept for Next-Gen IAM, building an open system that enables interactions between identity management systems across environments, promoting standards, API integrations and identity management as a service across all stacks (Filho, 2025).

2.3 Limitations of Traditional IAM Systems

Implementing Identity Access Management (IAM) is crucial for organizations to protect assets. Legacy systems are inadequate for today's needs. Legacy IAM solutions use static, rule-based access control lists (ACLs) with predefined rights, considering limited variables like user attributes, groups, time, and IP addresses. However, important variables like user behavior and real-time risk scores are missing, leading to security gaps or poor user experience. Legacy IAM solutions rely on a perimeter-based model assuming users inside the corporate network are trusted - an outdated assumption in today's cloud-based, work-from-home (WFH) world moving towards zero-trust. Despite warnings, users remain vulnerable to password phishing and credential stuffing attacks, while multi-factor authentication (MFA) can be breached through MFA fatigue. Managing user identity lifecycles is challenging, especially handling deleted or "orphaned" users whose accounts remain active. Legacy systems often grant users "accidental" authorizations during their lifecycle. Additionally, these solutions only authenticate users at initial application access, not

continuously. If an account is compromised, the IAM system remains unaware of subsequent attacks. These limitations make a strong case for evolving AI-based intelligent IAM solutions (Filho, 2025; Yuan et al., 2025; Odeyemi et al., 2024).

2.4 The Imperative for AI Integration

The purpose of this survey on the challenges of IAM systems was to deal with some of these challenges. In this paper we discuss how ML can convert IAM from the present rule based stiff approach to an adaptable, flexible and thus intelligent system. Modern ML techniques help in enabling continuous dynamic authentication, context-based risk driven access control and also in identity governance by analyzing patterns in authentication and access request data along with users' behavior. The following sections provide an in-depth view on how each of these AI techniques can help in enhancing the functionality of IAM systems (Filho, 2025; Lesavre, 2020).

3. Role of Artificial Intelligence in Identity Verification

Identity Verification in Identity and Access Management (IAM) verifies individuals' identities before granting access to resources such as files, systems or premises. Traditional verification methods use knowledge-based authentication like passwords and token-based authentication like one-time passcodes. However, these methods are ineffective against today's sophisticated attacks and user expectations. Artificial Intelligence (AI) transforms verification into a dynamic authentication process, moving from binary decisions to probability-based identity verification using multiple data points from various sources. Authentication becomes dynamic through core AI technology (Filho, 2025; Lesavre, 2020; Zhang et al., 2020).

3.1 From Static to Continuous Verification

Traditional identity verification practices follow a "once authenticated, always trusted" principle. After you have entered your password and confirmed with a second factor (2FA) your application considers you trusted for the remainder of your session. The time between session takeover and the next authentication is left unsecured. With the help of AI, continuous authentication replaces the initial authentication and AI engines in applications evaluate user behaviour throughout a session and assign a risk score. If unusual events such as a change in typing pattern, different login locations or access to sensitive information occur, the application may ask for additional verification steps, may require more authentications or may terminate the session. With a machine learning engine at the core, an application learns the user's behaviour from historical data and sets up a baseline based on the average authentication behaviour. This includes parameters such as time to access the application, the devices used and the user behaviour within the application. As soon as a change in the user behaviour is identified the application evaluates the risk of the session and allows the business to adjust the level of security and the user experience accordingly(Zhang et al., 2020).

Figure 1. Continuous Authentication – Key Data Sources

Figure .1 refers to the process of collecting three types of signals, i.e. behavioral biometrics (such as Keystroke, Mouse dynamics), device signals (device fingerprint and its components), contextual biometrics (location, time of access, network information). All these signals are then passed on to the Machine learning engine, which gives a real time risk score of the user and then further decides the

mode of authentication of the user based on the risk score and further actions to be taken at the time of a potential risk being detected (Filho, 2025).

3.2 AI-Driven Identity Verification Techniques

Artificial intelligence (AI) is often associated with identity verification. While not always accurate, this connection has merit. AI represents a distinct technology based on fundamentally different principles.

- **Behavioral Analytics**

Behavioral analytics solution uses machine learning techniques including Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks to analyze endpoint user behavior through keystroke, mouse, and touchscreen analysis. Unlike traditional biometric methods, our behavioral authentication technology continuously monitors user behavior without user action and provides instant verification during sessions transparently (Filho, 2025; Yuan et al., 2025; Odeyemi et al., 2024).

- **Risk-Based Adaptive Authentication**

Risk-Based Authentication uses machine learning classifiers to identify users based on contextual factors like device fingerprint, location, time and behavior patterns. A risk score is calculated in real time and access is granted or denied based on predefined rules. Low risk attempts are seamless, while higher risk attempts require secondary authentication to mitigate attacks like compromised passwords and brute force attacks(Odeyemi et al., 2024).

- **Document and Credential Verification**

Document Authentication uses Document Authenticity Analysis to detect forgeries, Liveness Detection to prevent photo/video attacks, and Face Matching to match document identity with the user's image/video during authentication. We apply Computer Vision with deep learning algorithms and Convolutional Neural Networks (CNNs) to facilitate user authentication during Onboarding(Yuan et al., 2025).

3.3 Comparative Overview of Verification Approaches

Feature	Traditional Verification	AI-Enabled Verification
Verification Timing	Point-in-time (login only)	Continuous (throughout session)
Decision Type	Binary (accept/reject)	Probabilistic (risk score-based)
User Interaction	Explicit (user must act)	Passive (transparent to user)
Adaptability	Static rules	Dynamic, learns from new data
Fraud Detection	Rule-based pattern matching	Anomaly detection via ML models
Scalability	Linear resource scaling	Automated, non-linear scaling

Table 1. Comparison of Identity Verification Approaches

3.4 Benefits and Challenges of AI-Enhanced Verification

Using AI in identity verification can bring a number of benefits such as proactive and continuous security monitoring; risk-based friction to ensure good user experience; Scalability in terms of the number of verifications that can be processed. But it also comes with challenges like unintended bias from biased datasets that affect certain groups of people in identity verification. The collection of users' behavioral and biometric data. Adversarial attacks on AI-based detection mechanisms. The lack of explainability of the AI's decision-making process, which makes auditing and compliance with regulations very challenging (Filho, 2025; Lesavre, 2020).

4. Enhancing Access Control with AI

Traditional access control models like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are not suitable for modern dynamic systems. These models are static and lack flexibility for complex access control scenarios in today's systems. Traditional models provide limited flexibility and do not support fine-grained contextual access control needed for dynamic risk environments and insider threats. They also lack scalability for distributed systems and cloud environments. Many security threats must be overcome (Atlam and Yang, 2025; Feng et al., 2008; Li et al., 2024). Conventional access control systems cannot make dynamic decisions based on context and risk-based authorization. The Contextual Risk Based Access Control (CRBAC) and Authorization Control models use real-time contextual risk indicators to evaluate access requests. They employ AI techniques and game-theoretic methods to assess requests based on user behavior, location, device state and access history, providing accurate authorization based on current security situations. As security situations vary with time, AI enables dynamic policy generation and optimization, providing continuous permission updates to minimize human errors and reduce administrative burden. AI is used for anomaly detection through machine learning to counter insider threats and unknown attacks not covered by rule-based systems, enhancing overall security posture (Li et al., 2024; Dhanushkodi and Thejas, 2024; Atlam and Yang, 2025).

Integration of AI in Zero Trust Architecture (ZTA) ensures access controls, continuous authentication and authorization, and least privilege access while eliminating implicit trust. ZTA leverages machine learning for threat intelligence, real-time anomaly detection and authentication automation. AI can analyze vast data in real-time to uncover attack patterns, ransomware and insider threats. The integration utilizes confidential computing and hardware-based Trusted Execution Environments (TEEs) to protect data. AI in ZTA provides robust security relevant for cloud and hybrid enterprise infrastructures, despite downsides of costs, complexity and user resistance (Ofili et al., 2025; Bashir, 2024; Atlam and Yang, 2025).

There are still many challenges to be solved in the field of AI and Access Control. Some of them are:

- Lack of Trust and Transparency: With the use of new complex AI models, the “black box” nature of the systems makes it more difficult to understand and trust the access control decision made by the system.
- Ethical, Privacy and Legal Challenges: The new ways of collecting and processing data in the context of AI-based access control, raise new ethical, privacy and legal challenges that need to be addressed.
- Interpretability and Explainability: Access control system users need to understand and be able to explain the decision made by the system, in order to be able to trust it.
- Scalability: Deep learning models are very difficult to scale in order to achieve real time response from the system, especially when dealing with large and dynamic datasets.

The integration of an AI-based access control system with legacy systems, as well as compliance with current standards and regulations, is not an easy task. Another challenge that is still an open research area is the protection of the AI model against adversarial attacks and the prevention of manipulating the access control system (Mylrea and Robinson, 2023; Dhanushkodi and Thejas, 2024; Nzeako and Shittu, 2024).

In summary, AI can be leveraged in order to achieve many benefits in access control such as eliminating several constraints in traditional authorization models, using context- and risk-based authorization, anomaly detection and policy optimization. Achieving a robust and sustainable Zero Trust Architecture by leveraging the power of AI for continuous risk-based automated access verification and threat intelligence are also many other benefits of adopting AI in access control. However, AI in access control has several unaddressed challenges such as explainability, ethics, and scalability, and also the

complexity of integration with legacy systems to achieve trustworthy AI in access control systems (Atlam and Yang, 2025; Li et al., 2024; Ofili et al., 2025; Mylrea and Robinson, 2023).

5. Privacy and Security Challenges in AI-enabled Identity Management

The use of Artificial Intelligence (AI) in identity management has led to a whole host of new privacy and security concerns. Today, more secure IAM solutions are using AI to authenticate users via biometric technology such as facial, speech and behavioral analysis. This is said to be more secure than traditional passwords. However, there are numerous new risks and challenges that have emerged as a result of the use of AI in identity management (Vegas and Llamas, 2024; Filho, 2025). With the growing adoption of AI in the identity verification (ID) industry, protecting biometric and behavioral data is a pressing concern. Biometric and behavioral data is inherently private, and any compromise of privacy could expose individuals to identity theft and loss of sensitive information. The purpose of the AI sitting on top of the ID is to protect against these risks, but there are significant privacy risks associated with the AI itself – including adversarial attacks, model inversion attacks and other forms of attacks that can be used to exploit the openness and complexity of the AI, and as a result leak the personal data it was put in place to protect – all of which could undermine the very identity verification process they are intended to secure (Al-Kharusi et al., 2024; Al-Khassawneh, 2022).

Although some privacy concerns discussed above remain relevant to modern AI-based Identity and Access Management (IAM) solutions, they also present several new privacy concerns that need to be addressed. Examples include GDPR and CCPA (Vegas and Llamas, 2024; Xu et al., 2022). One of the problems with modern AI-based systems is that they are generally opaque, and it is not always known how access decisions are made. To ensure that the required level of GDPR/CCPA transparency and accountability is achieved in modern AI-based IAM systems, methods such as explainable AI (XAI), federated learning, and differential privacy should be used to achieve the necessary visibility in the IAM systems and in the data flows (Ijaiya, 2024). These methods are especially important when the sensitive data is located at the distant ends of the training or processing of the AI models. In addition to all the previous requirements, we are dealing with new requirements, including dealing with emerging threats (such as anomalies and insider threats) and the use of AI-based identity management to achieve continuous risk-based decision making via analysis of patterns and anomalies. In addition, the AI-based system has to be resilient to attacks like poisoning, where attackers attempt to reduce the overall accuracy of the AI, and thus reduce the reliability of the AI-based system (Ijaiya, 2024; Xu et al., 2022).

We now have the challenge of balance. Balance between being open and being secure. Open-source models allow us to be more collaborative but in an open-source model there are many vulnerabilities such as membership inference attacks, and backdoor attacks which allows attackers to obtain personal identifiable information and allow attackers to gain access to systems, and so on (Rupanetti and Kaabouch, 2024). And we need to really develop countermeasures like differential privacy and adversarial training for the identity management space. The large-scale AI-based IAM in the future emerging scenarios such as cloud, industrial environment and 6G networks is of huge volume, low resource density, which may cause potential impacts on security performance. Therefore, intelligent and efficient AI-based security solutions for privacy protection and defense against new-generation cyber-attacks are in urgent need (Filho, 2025; Al-Khassawneh, 2022).

The use of new-generation, AI-based solutions for identity and access management (IAM) that facilitate faster user authentication, and authorization raises new challenges to privacy and security. These include the need to defend against AI-based attacks, protect biometric data, ensure compliance with data protection laws by using transparent and privacy-by-

design AI, and mitigate the ongoing threats from diverse types of attacks through dynamic defense mechanisms. To ensure the secure development of innovative AI-based IAM solutions, appropriate technical, ethical and regulatory measures need to be implemented within a collaborative governance framework (Vegas and Llamas, 2024; Filho, 2025; Al-Kharusi et al., 2024; Ijaiya, 2024; Al-Khassawneh, 2022).

6. Ethical and Regulatory Considerations

Ethical and regulatory questions arise regarding AI-based identity management. Biometric identification systems significantly impact individuals and society. Key ethical concerns include privacy, bias, transparency, accountability, and respect for human autonomy. Brendel et al. (2021) highlight problems caused by complex autonomous technologies and suggest ethical frameworks consider micro- and macro-environments. Data privacy is crucial for many applications. AI-based identity systems handling biometric and behavioral data must address privacy through methods like differential privacy, federated learning, and homomorphic encryption while maximizing AI use and promoting trust. This includes compliance with GDPR and other global laws (Abolaji and Akinwande, 2024; Radanliev et al., 2024). Bias and discrimination persist in many systems. If training data fails to reflect population diversity, AI will discriminate against minorities and identity verification will worsen this issue. XAI models will provide accountability through visibility of the black box, allowing users and regulators to assess decisions made by AI systems. In finance, healthcare or education these decisions are critical and require explanation (Selvam and Vallejo, 2025) (Amini et al., 2023). Beyond technology, legal measures for AI must address its challenges. The proposed EU AI Act and future global versions will ensure AI follows principles of fairness, accountability, transparency and responsibility, including algorithmic accountability, data ownership, liability and non-harassment rules. The international community has already faced challenges with harmonizing national regulatory approaches (Dokumacı, 2024). To implement identity management with AI, governance must ensure compliance can be reviewed and verified. Regulatory issues must be considered early in technology development, requiring cooperation between politicians, engineers and ethicists (Thoom, 2025).
The key challenge for the ethics and regulation of IDMS is to develop new technologies that effectively and innovatively protect basic values such as privacy, non-discrimination, transparency and accountability, and that therefore also enable the safe development and use of ICT. This requires the development and implementation of ethical management frameworks, privacy-preserving AI methods, compliance with new regulations (such as GDPR and the AI Act), and multidisciplinary governance models (Brendel et al., 2021; Abolaji and Akinwande, 2024; Dokumacı, 2024; Radanliev et al., 2024; Gilbert and Gilbert, 2024).

7. Conclusion and Future Directions

This survey report describes the findings of the first-of-its-kind Artificial Intelligence (AI) in Identity and Access Management (IAM) Survey. It gathered information regarding the role of AI in modern IAM systems and solutions and revealed that the IAM industry has gone through a significant transformation from a static, rule-based security model to a dynamic, adaptive, and intelligent security model (Rane and Paramesha, 2024). The survey found that AI is highly effective in the fields of identity verification, biometrics and access control. It provides continuous authentication through the means of behavioral biometrics, risk-based access decisions by using real-time data and context-based access decisions by leveraging on the principles of zero-trust architecture. The adoption of AI in IAM brings about numerous benefits but also introduces new sets of challenges including algorithmic bias, privacy exposures, advanced attacks and the lack of visibility into the working mechanisms of AI-based systems. Some of the key recommendations for future work on AI-based IAM solutions that emerged from

this survey include Explainable AI (XAI) to ensure that all authentication and authorization decisions can be audited (Malik, 2024; Zhang et al., 2024; Benmalek et al., 2022). The explainability of the authentication and authorization decisions is crucial to ensure that today's opaque machine learning-based IAM solutions are auditable. Privacy-preserving technologies such as federated learning and homomorphic encryption to train AI-based IAM systems securely without exposing users' sensitive personal identity information (PII). Combating Adversarial Attacks - modern day attacks are evolving and AI-based IAM systems must be trained to be resilient to such attacks. Raising awareness and enforcing compliance with AI-centric regulations as well as harmonizing existing regulations (e.g., GDPR) with the evolving trends in AI for IAM (Rane et al., 2024).

8. References

1) Mishra, A. (2024). A Comprehensive Review of Artificial Intelligence and Machine Learning : Concepts, Trends, and Applications. International Journal of Scientific Research in Science and Technology, 11(5), 126–142. https://doi.org/10.32628/ijsrst2411587
2) Basak, S., Chatterjee, P., Biswas, D., Bhadra, P., & Das, R. (2024). Introduction to AI and ML Technologies and Their Potential Applications in Cybersecurity (pp. 277–309). Igi Global. https://doi.org/10.4018/979-8-3693-6557-1.ch012
3) Filho, W. L. R. (2025). THE ROLE OF AI IN ENHANCING IDENTITY AND ACCESS MANAGEMENT SYSTEMS. International Seven Journal of Multidisciplinary, 1(2). https://doi.org/10.56238/isevmjv1n2-011
4) Yuan, F., Zuo, Z., Jiang, Y., Shu, W., Tian, Z., Ye, C., Yang, J., Mao, Z., Huang, X., Gu, S., & Peng, Y. (2025). AI-Driven Optimization of Blockchain Scalability, Security, and Privacy Protection. Algorithms, 18(5), 263. https://doi.org/10.3390/a18050263
5) Lesavre, L. (2020). A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. National Institute Of Standards Technology. https://doi.org/10.6028/nist.cswp.01142020
6) Zhang, H., Bosch, J., & Olsson, H. H. (2020). Federated Learning Systems: Architecture Alternatives. 385–394. https://doi.org/10.1109/apsec51365.2020.00047
7) Odeyemi, O., Okoye, C., Ofodile, O., Adeoye, O., Addy, W., & Ajayi-Nifise, A. (2024). INTEGRATING AI WITH BLOCKCHAIN FOR ENHANCED FINANCIAL SERVICES SECURITY. Finance & Accounting Research Journal, 6(3), 271–287. https://doi.org/10.51594/farj.v6i3.855
8) Dhanushkodi, K., & Thejas, S. (2024). AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation. IEEE Access, 12, 173127–173136. https://doi.org/10.1109/access.2024.3493957
9) Mylrea, M., & Robinson, N. (2023). Artificial Intelligence (AI) Trust Framework and Maturity Model: Applying Entropy Lens to Improve Security, Privacy, and Ethical AI. Entropy, 25(10), 1429. https://doi.org/10.3390/e25101429
10) Feng, F., Lin, C., Peng, D., & Li, J. (2008). A Trust and Context Based Access Control Model for Distributed Systems. 9, 629–634. https://doi.org/10.1109/hpcc.2008.37
11) Bashir, T. (2024). Zero Trust Architecture: Enhancing Cybersecurity in Enterprise Networks. Journal of Computer Science and Technology Studies, 6(4), 54–59. https://doi.org/10.32996/jcsts.2024.6.4.8
12) Nzeako, G., & Shittu, R. (2024). Leveraging AI for enhanced identity and access management in cloud-based systems to advance user authentication and access control. World Journal of Advanced Research and Reviews, 24(3), 1661–1674. https://doi.org/10.30574/wjarr.2024.24.3.3501
13) Ofili, B., Erhabor, E., & Obasuyi, O. (2025). Enhancing federal cloud security with AI: Zero trust, threat intelligence and CISA Compliance.

World Journal of Advanced Research and Reviews, 25(2), 2377–2400. https://doi.org/10.30574/wjarr.2025.25.2.0620
14) Li, B., Yang, F., & Zhang, S. (2024). Context-Aware Risk Attribute Access Control. Mathematics, 12(16), 2541. https://doi.org/10.3390/math12162541
15) Filho, W. L. R. (2025). THE ROLE OF AI IN ENHANCING IDENTITY AND ACCESS MANAGEMENT SYSTEMS. International Seven Journal of Multidisciplinary, 1(2). https://doi.org/10.56238/isevmjv1n2-011
16) Al-Kharusi, Y., Khan, A., Rizwan, M., & Bait-Suwailam, M. (2024). Open-Source Artificial Intelligence Privacy and Security: A Review. Computers, 13(12), 311. https://doi.org/10.3390/computers13120311
17) Al-Khassawneh, Y. A. (2022). A Review of Artificial Intelligence in Security and Privacy: Research Advances, Applications, Opportunities, and Challenges. Indonesian Journal of Science and Technology, 8(1), 79–96. https://doi.org/10.17509/ijost.v8i1.52709
18) Vegas, J., & Llamas, C. (2024). Opportunities and Challenges of Artificial Intelligence Applied to Identity and Access Management in Industrial Environments. Future Internet, 16(12), 469. https://doi.org/10.3390/fi16120469
19) Ijaiya, H. (2024). Harnessing AI for data privacy: Examining risks, opportunities and strategic future directions. International Journal of Science and Research Archive, 13(2), 2878–2892. https://doi.org/10.30574/ijsra.2024.13.2.2510
20) Xu, Q., Su, Z., & Li, R. (2022). Security and Privacy in Artificial Intelligence-Enabled 6G. IEEE Network, 36(5), 188–196. https://doi.org/10.1109/mnet.117.2100730
21) Brendel, A. B., Mirbabaie, M., Lembcke, T.-B., & Hofeditz, L. (2021). Ethical Management of Artificial Intelligence. Sustainability, 13(4), 1974. https://doi.org/10.3390/su13041974
22) Mohammad Amini, M., Jesus, M., Fanaei Sheikholeslami, D., Alves, P., Hassanzadeh Benam, A., & Hariri, F. (2023). Artificial Intelligence Ethics and Challenges in Healthcare Applications: A Comprehensive Review in the Context of the European GDPR Mandate. Machine Learning and Knowledge Extraction, 5(3), 1023–1035. https://doi.org/10.3390/make5030053
23) Abolaji, E., & Akinwande, O. (2024). AI powered privacy protection: A survey of current state and future directions. World Journal of Advanced Research and Reviews, 23(3), 2687–2696. https://doi.org/10.30574/wjarr.2024.23.3.2869
24) Dokumacı, M. (2024). Legal Frameworks for AI Regulations. Human Computer Interaction, 8(1), 133. https://doi.org/10.62802/ytst2927
25) Selvam, M., & González Vallejo, R. (2025). Ethical and Privacy Considerations in AI-Driven Language Learning. LatIA, 3, 328. https://doi.org/10.62486/latia2025328
26) Radanliev, P., Santos, O., Brandon-Jones, A., & Joinson, A. (2024). Ethics and responsible AI deployment. Frontiers in Artificial Intelligence, 7. https://doi.org/10.3389/frai.2024.1377011
27) Gilbert, C., & Gilbert, M. A. (2024). The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations. International Journal of Scientific Research and Modern Technology (IJSRMT), 3(9), 9–17. https://doi.org/10.38124/ijsrmt.v3i9.45
28) Thoom, S. (2025). Lessons from AI in finance: Governance and compliance in practice. International Journal of Science and Research Archive, 14(1), 1387–1395. https://doi.org/10.30574/ijsra.2025.14.1.0235
29) Rane, N. L., & Paramesha, M. (2024). Explainable Artificial Intelligence (XAI) as a foundation for trustworthy artificial intelligence. Deep Science. https://doi.org/10.70593/978-81-981367-4-9_1
30) Malik, D. P. (2024). Scalability and Robustness of Federated Learning Systems: Challenges and Solutions. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING

AND MANAGEMENT, 08(06), 1–5. https://doi.org/10.55041/ijsrem35575

31) Zhang, Y., Zeng, D., Luo, J., Fu, X., Chen, G., Xu, Z., & King, I. (2024). A Survey of Trustworthy Federated Learning: Issues, Solutions, and Challenges. ACM Transactions on Intelligent Systems and Technology, 15(6), 1–47. https://doi.org/10.1145/3678181
32) Benmalek, M., Benrekia, M. A., & Challal, Y. (2022). Security of Federated Learning: Attacks, Defensive Mechanisms, and Challenges. Revue d'Intelligence Artificielle, 36(1), 49–59. https://doi.org/10.18280/ria.360106
33) Rane, J., Kaya, Ö., Mallick, S. K., & Rane, N. L. (2024). Artificial intelligence, machine learning, and deep learning in cloud, edge, and quantum computing: A review of trends, challenges, and future directions. Deep Science. https://doi.org/10.70593/978-81-981271-0-5_1

