

Assignment1.docx

by Iznah Hasbullah

Submission date: 27-Jul-2025 10:56PM (UTC+0800)

Submission ID: 2721168947

File name: Assignment1.docx (27.97K)

Word count: 2039

Character count: 12903

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 28 June 2025

Hand-in Date: 12 July 2025

Hand-in Method: Online Submission via E-Learning.

Assignment Report: Artificial Intelligence and Identity Access Management

Table of contents:

- Summary research paper's
- Critical Analysis:
- Connections
- Conflicts between the findings
- Synthesis Matrix for Literature Review:
- References

Summary research papers:

Paper 1: Identity Management Capability Powered by Artificial Intelligence

⁵ This paper provides a review of how AI powers identity management to allow easy user access privileges. Artificial Intelligence (AI) reshapes enterprises and organizes innovation management. AI may force management, consistent with fast technological progress and the replacement of human organization, to reconsider the whole process of innovation of a business. IAM systems offer administrators tools and technology to alter user roles, monitor user activity, provide reports, and continuously implement rules [1]. These systems are developed to offer a method of managing user access throughout a company and to guarantee that corporate rules and government laws are complied with. Identity management's overall objective is to provide access to company assets for which individuals and devices are entitled in a certain situation [2]. This covers onboarding users and systems, authorization, and prompt offboarding of users and devices (Ishaq Azhar Mohammed 2021)

Paper 2: Artificial Intelligence Enhanced IAM Preventing Unauthorized Access in Modern Enterprises

⁴ As enterprises increasingly migrate to digital platforms, securing systems from unauthorized access becomes crucial to safeguarding sensitive data. Identity and Access Management (IAM) systems have traditionally been implemented to manage user access and authenticate identities. However, with growing threats of sophisticated cyber-attacks, traditional IAM methods are proving inadequate. Artificial Intelligence (AI) has emerged as a transformative force in enhancing IAM systems by providing adaptive, intelligent solutions to prevent unauthorized access. This paper explores the role of AI-enhanced IAM in modern enterprises, emphasizing its ability to predict, detect, and respond to potential security breaches. Through a detailed examination of current AI applications in IAM, this study demonstrates how AI-enabled tools can increase security resilience, reduce false positives, and automate responses to evolving threats, thus offering enterprises a proactive defense against unauthorized access. (Md Takbir Sarker, Md Sanaur Rahman, Mohammed Mahi Uddin, Nur Alam Farhad Shakil, 2024)

Paper 3: ⁷ Artificial Intelligence-based Access Management System

³ The foundation of cybersecurity is identity and access management (IAM). Its methods, procedures, and guidelines control identity access to digital resources and define the scope of identity permission over the resources. A significant number of data breaches are caused by ineffective security features, software vulnerabilities, human error, malicious insiders, and the misappropriation of access and privileges. Artificial intelligence (AI) techniques can upgrade the access management system. As a result, research into artificial intelligence in IAM is required to enable organizations to take a more detailed and flexible approach to authentication and access control to mitigate cyber threats and other IAM challenges. This study explores the relationship between access management systems and artificial intelligence with regard to AI applications in identity and access management, specifically the monitoring, administration, and control of access privileges. The objective of this study was to provide evidence from the relevant literature to help understand how AI works in mitigating identified IAM challenges. The findings in this study demonstrate how artificial intelligence strengthens identity and access management in mitigating growing cyber threats, automating processes, and keeping up with technological advancements. (Victoria Adenola, 2023)

Paper 4: ⁸ Machine learning in identity and access management systems: Survey and deep dive

¹ The evolution of identity and access management (IAM) has been driven by the expansion of online services, cloud computing, and the Internet of Things (IoT). The proliferation of remote work, mobile applications, and interconnected devices has intensified the demand for robust identity protection and access control. As digital interactions and data sharing become more prevalent across industries, IAM has gained prominence, compelled by the need to safeguard sensitive information, prevent unauthorized access, and adhere to increasingly stringent regulatory frameworks. In parallel with IAM's evolution, the integration of artificial intelligence (AI) has emerged as a pivotal avenue for enhancing IAM effectiveness. This survey delves into the fusion of machine learning (ML) techniques to fortify IAM, with a specific focus on its core processes: authentication, authorization, and auditing. Addressing fundamental questions regarding ML's role in enhancing IAM processes, we begin by proposing a comprehensive definition of IAM within a unified layered reference model, highlighting Authentication, Authorization, and Auditing functions (with focus on monitoring). Furthermore, our survey comprehensively explores ML-based solutions within IAM systems, presenting a taxonomy of state-of-the-art methodologies categorized by their application in IAM processes. Drawing from both qualitative and quantitative insights from cited references, we investigate how ML enhances the performance and security of IAM processes. Additionally, by investigating challenges in implementing ML in IAM systems, we shed light on issues such as data privacy concerns and the interpretability of ML-driven decisions. In conclusion, this paper makes a substantial contribution to the IAM landscape by providing comprehensive insights into the transformative role of ML. Addressing pivotal questions, our survey offers a roadmap to leverage ML's potential for enhancing the performance, security, and efficacy of IAM systems. (Aboukadri SOuaddah AMezrioui A 2024)

Paper 5: ² How AI can improve identity verification and access control processes

² Artificial intelligence (AI) is recognized as the driving force responsible for reinventing a wide range of industries, among them IAM. This paper, therefore, looks for the potential for advancement in AI systems with respect to IAM, focusing on identity verification and access control within IAM systems. IAM systems face really difficult problems nowadays: management of user identity, real-time access control, and protection from modern threats. Traditional approaches have proven to be inefficient worldwide because of the static nature of the approaches and the lack of human intervention. In this way, this work provides a discussion on how these IAM challenges are to be effectively managed with the application of AI technologies. AI empowers strong tools of advanced data analytics, machine learning mechanisms, and automation. Equipped with all these capabilities, IAM systems can monitor user activity and behavior continuously, identify emerging anomalies in real time, and dynamically enforce policies to greatly enhance security and efficiency. Research has shown that AI brings better results in terms of security and productivity and offers scalable solutions in light of current and future needs for identity management. AI integration can streamline the process of verification of identity, offer enhanced mechanisms of authentication that are enhanced, and deliver precise and dynamic access control methods. Meanwhile, resonant incorporation of AI in IAM definitively gives the systems the ability to learn and change and to learn firm protection along with operational resilience against threats that constantly change over time. In this light, IAM systems based on AI will be able to properly satisfy the growing demands of modern organizations in terms of proper security, optimum performance, and user satisfaction..(Sri kanth Mandru 2022)

Paper 6: ⁶ Research on security protection technology of terminal access network based on fingerprint perception and identity protection of artificial intelligence

⁶ This paper proposes a kind of security protection measures such as vulnerability detection and identity authorization management for the equipment and transmission network segments based on the existing terminal access network field equipment and transmission network segments by using fingerprint sensing technology and identity protection technology, combined with advanced technologies such as artificial intelligence, big data processing and Internet of Things technology. It will further enhance the safety and reliability of Internet of Things equipment, provide equipment managers with the basis for formulating accurate safety management plans, and provide effective guarantee for the safety of existing terminal access network equipment. (Shu FZhang KLuo CMa BChen S 2020)

Critical Analysis:

Strengths and shortcomings are included in the research on Artificial Intelligence and Identity Access Management. The papers take an approach to addressing a pertinent security issue by using artificial intelligence technologies in the field of Identity Access Management. Research on Artificial Intelligence and Identity Access Management is more practically relevant when scalability and practical applicability are considered. However, the use of AI is very important but faces some challenges, including ensuring data privacy, mitigating algorithmic bias, and integrating AI with existing systems. Other key challenges are maintaining consistency, ensuring explainability and auditability of AI decisions, adapting to change, and managing privilege creep. It would be improved for managing AI-driven identities, permissions, and access control.

Connections:

- 1- **Focus on AI on IAM:** Focusing on managing identities and access management is extremely important in our current era, especially through the use of artificial intelligence.
- 2- **Limitation of traditional IAM:** All papers agreed that traditional use is no longer as effective as AI in tackling the risks associated with identity and access management.
- 3- Core IAM functions by using AI:
 - Authentications
 - Authorizations
 - Access control management
 - Auditing
- 4- **The Use of ML:** Automating processes through the use of artificial intelligence.

Conflicts between the findings:

- 1- **Integration Scope:** Full integration between AI and IAM on pages 2 and 5.
Conflict: Other pages to be integrated gradually.
- 2- **Security and Privacy:** This is emphasized on page 5 to improve security and monitor user behavior.
Conflict: With page 4 because intensive monitoring may violate user privacy.
- 3- **Trust and Decision:** The Policy implementation through artificial intelligence is carried out automatically without human intervention, on Pages 5 and 2.
Conflict: There is a difference in who trusts the decisions of artificial intelligence on the page.
- 4- **Automation vs. Human Intervention:** On page 2, encourage the automation of action taking.
Conflict: Contradicts page 6 on the importance of human intervention, especially for sensitive systems.

Synthesis Matrix for Literature Review:

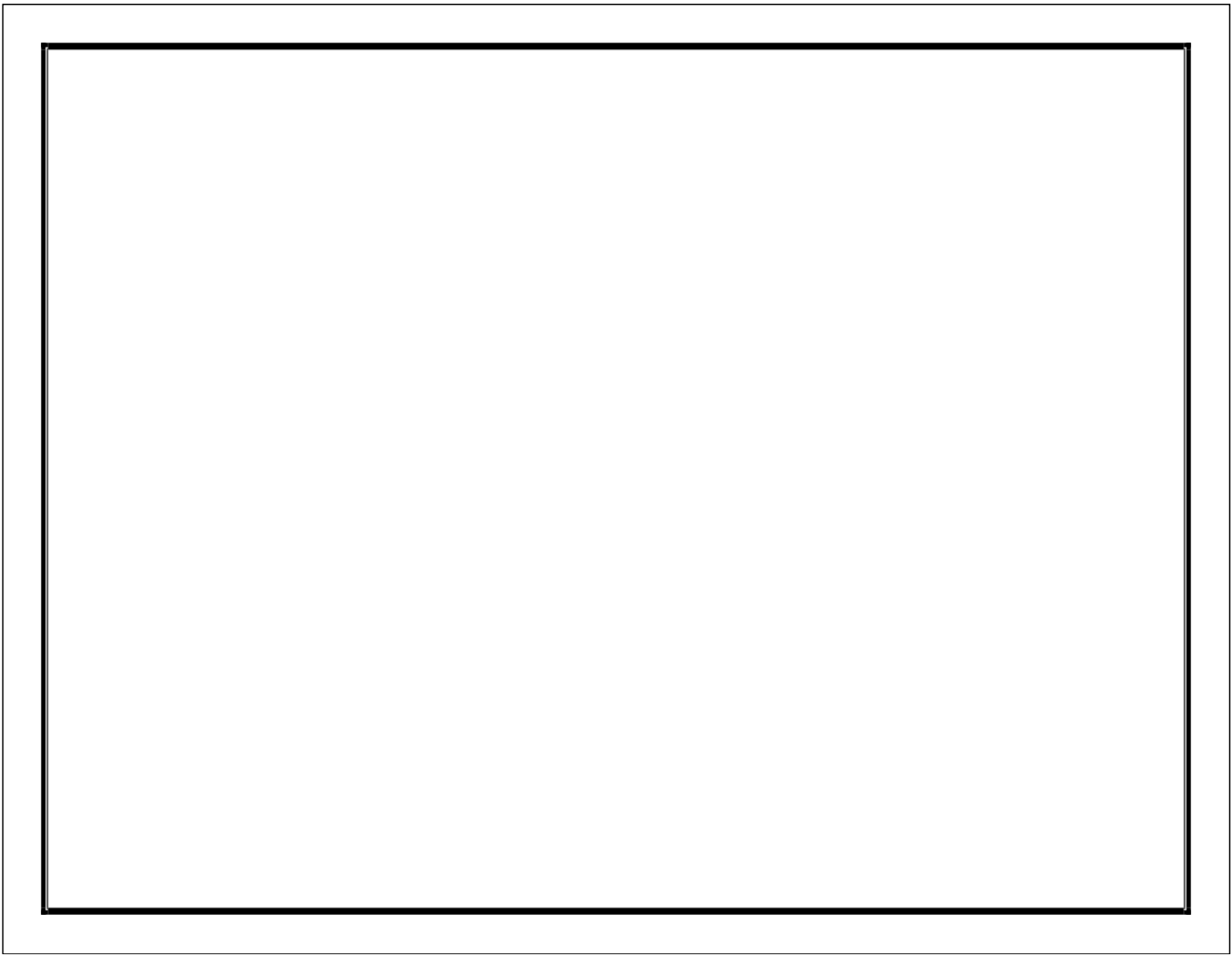
Study	Authors	Year	Research Design	Key Findings/Results	Methodology	Limitations
Paper 1: The possibility of using identities using AI	Ishaq Azhar Mohammed	2021	Literature Review	Artificial intelligence is reshaping identity and access management (IAM) by automating access, monitoring, and policy enforcement	Comprehensive analysis of the integration of artificial intelligence into identity and access management processes	Lack of experimental validation and implementation insights
Paper 2: Improving Identity and Access Management with AI in Modern Enterprises	Md Takbir Sarker, Md Sanaur Rahman, Mohammed Mahi Uddin, Nur Alam Farhad	2024	Analytical & Review Study	AI increases identity and access management by reducing false positives and automates breach responses.	Exploring cases and comparing the use of artificial intelligence in identity and access management	Incomplete ability to address data governance and AI interpretability

	Shakil					
7 Paper 3: AI-Based Access Management System	Victoria Adenola	2023	Literature Review	AI addresses identity and access management challenges such as insider threats, human errors, and software flaws; it also enhances resilience and control by using access based on role.	Conceptual analysis with support from prior studies	Comprehensive scope; lacks focus on specific AI technologies used
Paper 4: ML in IAM Systems – Survey	Aboukadri SOuaddah A Mezrioui A	2024	Survey Paper	ML improves authentication, authorization, and auditing	In-depth survey with proposed reference model and classification	Privacy and interpretability challenges in ML have not been deeply resolved
Paper 5: Artificial Intelligence Contributes to the Identity Verification	Sri kanth Mandru	20222	Conceptual/Analytical	Artificial intelligence enables real-time monitoring, anomaly detection, and	Discussion and analysis of the capabilities of artificial intelligence in identity and	Seamless integration, but ignores dealing with legacy systems

Process				adaptive access policies.	access management	
Paper 6: AI-Based Security in IoT Access	Shu FZhang KLuo CMa BChen S	2020	Technical Proposal	Combines AI, fingerprint sensing, and IoT for identity protection and vulnerability management.	Applied research using artificial intelligence, the Internet of Things, and fingerprint sensing integration	Handling peripheral equipment; not directly generalizable to broader IAM systems

References:

- Ishaq Azhar Mohammed. (2021) Identity Management Capability Powered by Artificial Intelligence to Transform the Way User Access Privileges Are Managed, Monitored, and Controlled. <https://www.mendeley.com/catalogue/23d2fdff-7e49-361f-b8d4-95af10979ee6/>
- Md Takbir Sarker, Md Sanaur Rahman, Mohammed Mahi Uddin, Nur Alam Farhad Shakil. (2024) Artificial Intelligence Enhanced Identity and Access Management Preventing Unauthorized Access in Modern Enterprises. <https://doi.org/10.62304/ijmisds.v1i04.202>
- Victoria Adenola.(2023). Artificial Intelligence-Based Access Management System. [DOI:10.13140/RG.2.2.24266.34243](https://doi.org/10.13140/RG.2.2.24266.34243)
- Aboukadri SOuaddah AMezrioui A. (2024). Machine learning in identity and access management systems: Survey and deep dive. <https://doi.org/10.1016/j.cose.2024.103729>
- Sri kanth Mandru. (2022). How AI can improve identity verification and access control processes. [DOI:10.47363/JAICC/2022\(1\)E101](https://doi.org/10.47363/JAICC/2022(1)E101)
- Shu FZhang KLuo CMa BChen S. (2020). Research on security protection technology of terminal access n based on fingerprint perception and identity protection of IoT. [DOI: 10.1109/ICIBA50161.2020.927715](https://doi.org/10.1109/ICIBA50161.2020.927715)



ORIGINALITY REPORT

62%
SIMILARITY INDEX

47%
INTERNET SOURCES

34%
PUBLICATIONS

27%
STUDENT PAPERS

PRIMARY SOURCES

1	Sara Aboukadri, Aafaf Ouaddah, Abdellatif Mezrioui. "Machine Learning in Identity and Access Management Systems: Survey and Deep Dive", Computers & Security, 2024 Publication	15%
2	www.onlinescientificresearch.com Internet Source	15%
3	thescholarship.ecu.edu Internet Source	10%
4	globalmainstreamjournal.com Internet Source	7%
5	www.researchgate.net Internet Source	7%
6	open-measure.atlassian.net Internet Source	6%
7	Adenola, Victoria. "Artificial Intelligence Based Access Management System", East Carolina University, 2023 Publication	2%

Exclude quotes

Off

Exclude matches

Off

Exclude bibliography

On