International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Review Article)

# Big data and machine learning for securing identity and access management systems

Nikhil Ghadge *

*Identity Services & Governance, Engineering Department, Okta. Inc,*

International Journal of Science and Research Archive, 2025, 15(01), 1198-1204

Publication history: Received on 11 March 2025; revised on 19 April 2025; accepted on 21 April 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.15.1.1115

## Abstract

In an era of expanding digital interconnectivity, the security of Identity and Access Management (IAM) systems has become a pivotal concern. This study explores the transformative potential of integrating big data analytics and machine learning technologies into IAM frameworks to address contemporary cybersecurity challenges. By examining the historical evolution and core functions of IAM systems, the research underscores their importance in managing digital identities and regulating access across complex infrastructures. The paper delves into various facets of big data processing—collection, storage, anomaly detection, real-time monitoring—and evaluates how machine learning techniques such as predictive analytics, adaptive access control, and user behavior analysis can fortify IAM against sophisticated cyber threats. Further, it investigates practical implementations, real-world applications, and challenges including data privacy, compliance, model interpretability, and scalability. Through a critical synthesis of recent literature and applied case studies, this research offers strategic insights and recommendations for deploying AI-driven IAM systems that are secure, adaptive, and scalable, positioning them as critical enablers of trust in modern digital ecosystems.

**Keywords:** Identity and Access Management; Big Data; Threat detection; Identity theft; Artificial Intelligence

## 1. Introduction

### 1.1. Background of Identity and Access Management Systems

Identity and access management (IAM) frameworks are pivotal in safeguarding sensitive data and resources in institutions. These frameworks are structured to facilitate the overseeing and regulation of digital identities and control access to diverse applications and systems. The roots of IAM trace back to the early eras of computing when user credentials and permissions were manually handled by administrators. As technology progressed, IAM frameworks evolved into more complex entities integrating functionalities like single sign-on, multi-factor authentication, and role-based access control. These innovations significantly bolstered organizations' security stance by enabling centralized management of user identities and access privileges. Nevertheless, in light of the increasing prevalence of big data and machine learning technologies, IAM systems confront fresh hurdles in conforming to the volatile threat landscape [1]. The amalgamation of these cutting-edge technologies into IAM frameworks can empower institutions to promptly identify and counter security menaces, further reinforcing their cybersecurity mechanisms against malevolent elements. Additionally, machine learning algorithms can be utilized to scrutinize user behavior trends and pinpoint unusual activities that could hint at a security breach. Gaining insight into the historical underpinnings of IAM frameworks and the probable advantages of integrating big data and machine learning, institutions can proactively enhance their security posture and alleviate the perils linked with unauthorized access and data breaches.

[*] Corresponding author: Nikhil Ghadge

### 1.2. Significance of Securing Identity and Access Management Systems

Within the domain of advanced technological frameworks, the security of Identity and Access Management (IAM) structures emerges as a preeminent concern requiring detailed attention and strategic execution. As conventional power grids transition into Smart Grids (SGs) enabled by the Internet of Things (IoT) [2], the interconnected essence of these structures accentuates the vital requirement for strong identity and access management. The intricacies inherent in IoT-supported SG frameworks highlight the urgent need to protect identities and manage access to guarantee the stability and dependability of the grid. Furthermore, as dialogues touch on a range of cybersecurity factors, such as infrastructure management, cyber defense tactics, and technological enhancement [3], it is evident that fortifying IAM structures is not solely a technical prerequisite but a multifaceted undertaking necessitating proactive actions and cooperation across scholarly circles. Hence, within the realm of cutting-edge innovations like big data and machine learning, the importance of enhancing the security of IAM systems resonates deeply as a foundational element supporting the strength and resilience of interconnected infrastructures.

### 1.3. Overview of Big Data and Machine Learning

Within the domain of identity and access management (IAM) systems, a profound comprehension of big data and machine learning holds paramount significance. The emergence of social machines has been a pivotal subject of discussion, fundamentally altering the dynamics of collective curation and memory accumulation, underscoring the pivotal role of digital platforms in sculpting social identity. Moreover, the trials presented by the diversity of big data, as articulated in [4], call for cutting-edge methodologies such as Dimensional Data Analysis (DDA) for the effective interpretation of intricate data frameworks. Through the utilization of DDA and analogous tools, enterprises can bolster their capacity to navigate and scrutinize extensive datasets, enabling the detection of anomalies and the optimization of security protocols. This fusion of machine learning with big data techniques not only expedites data comprehension but also opens avenues for advanced analytics in fortifying IAM strategies.

### 1.4. Research Aim and Objectives

The primary purpose of this study is to delve into the intricate realm of fortifying identity and access management systems using the amalgamation of big data and machine learning technologies. This scholarly investigation is set to pursue multiple aims. To start with, the study endeavors to scrutinize the contemporary landscape of identity and access management systems deployed by various organizations, with the intention of pinpointing prevalent weaknesses and risks. Such an endeavor is anticipated to furnish a holistic comprehension of the prevailing challenges necessitating rectification. Subsequently, the study aspires to delve into the realm of big data analytics to discern its potential in heightening the security stature of these systems, particularly by uncovering irregularities and trends that signify potential cyber intrusions. Through harnessing the prowess of machine learning algorithms, the study also looks forward to crafting prognostic models for preemptive identification and remediation of looming threats. Lastly, the study sets out to assess the efficacy of these methodologies in authentic scenarios, thereby proffering suggestions for bolstering the security fabric of identity and access management systems. By realizing these objectives, this study is primed to furnish invaluable insights to the domain of cybersecurity.

## 2. Role of Big Data in Securing Identity and Access Management Systems

### 2.1. Data Collection and Storage

Within the domain of safeguarding Identity and Access Management Systems, the amalgamation of Cyber-Physical Systems (CPS) and the Internet of Things (IoT) brings forth notable hurdles to traditional data gathering and retention methodologies. The dynamic nature of cloud-driven technologies requires a reassessment of data governance and confidentiality protocols as systems undergo real-time reconfigurations, potentially jeopardizing user privacy. The preservation of security, confidentiality, and dependability emerges as pivotal focal points within cloud computing environments, particularly when user data migrates to cloud platforms, introducing it to novel susceptibilities. To effectively tackle these quandaries, an astute integration of contemporary cryptographic protocols within cloud-based services and deployment structures holds utmost importance. An exhaustive examination of the repercussions associated with data accumulation, retention, and fortification concerning identity management underscores the urgency for resilient privacy-enhancing mechanisms amid the transforming technological terrains.

### 2.2. Data Processing and Analysis

The utilization of big data and machine learning for fortifying identity and access management systems hinges upon the pivotal role played by data processing and analysis. The magnitude, velocity, and diversity of data engendered by these systems mandate the employment of sophisticated methodologies for data handling and extraction of valuable insights.

Data processing encompasses activities like purging, reshaping, and warehousing data in a manner conducive to scrutiny. Subsequently, machine learning algorithms are harnessed to unearth patterns, irregularities, and interrelations within the dataset, thereby facilitating prognostic modeling and real-time decision-making. This recursive sequence of data processing and analysis enables entities to preemptively pinpoint security menaces, surveil user conduct, and bolster general system robustness. By amalgamating cutting-edge data processing methodologies with the capacities of machine learning, entities can reinforce their identity and access management systems to efficaciously safeguard confidential information and thwart illicit entry. Moreover, the continual assessment and enhancement of data processing and analysis techniques are imperative for acclimatizing to evolving cybersecurity risks and warranting the efficacy of security protocols .

### 2.3. Anomaly Detection

The utilization of machine learning methods has demonstrated considerable effectiveness in improving security within identity and access management systems by detecting anomalies. Existing research has pointed out the utilization of ML techniques within self-organizing cellular networks [5] and wireless networks [6], showcasing their potential in dealing with intricate network structures and facilitating adaptive decision-making processes. By harnessing supervised, unsupervised, reinforcement, and deep learning algorithms, researchers have been able to effectively process large datasets for anomaly detection, precise parameter estimation, and intelligent decision-making within dynamic environments. The examination of ML algorithms within heterogeneous networks, cognitive radios, and IoT applications further emphasizes their capacity to enhance security measures across varied network landscapes. Through an in-depth comprehension and application of diverse ML algorithms, organizations can prospectively detect and address anomalies within their identity and access management systems, thereby optimizing security procedures to safeguard critical information efficiently.

### 2.4. Predictive Analytics

Amidst the intricate realm of identity and access management systems, there is a growing recognition of the significance of predictive analytics as a pivotal element to fortify security measures and manage risks effectively [7]. The utilization of AI-driven algorithms, as showcased in [8], has the potential to revolutionize the detection and prevention of fraudulent activities within the banking domain. This approach facilitates instantaneous evaluations of credit applications, leading to the optimization of laborious processes. The notion of Algorithmic Jim Crow, expounded upon in [9], highlights the conceivable repercussions of biased algorithms in screening procedures, emphasizing the covert discriminatory effects that could arise from the application of ostensibly fair yet segregated vetting practices. Through the incorporation of predictive analytics into the fabric of identity management frameworks, organizations can capitalize on data-centric insights to preemptively counter security vulnerabilities and uphold the confidentiality of sensitive data. This progressive shift paves the way for a modern era characterized by resilient and streamlined access control mechanisms.

### 2.5. Real-time Monitoring

The role of real-time monitoring is vital in enhancing the security of identity and access management systems. The continuous monitoring of user activities enables swift detection and response to suspicious or unauthorized actions by system administrators. Immediate actions can be taken to address security threats before they evolve into more severe incidents. By harnessing big data and machine learning technologies, organizations can analyze extensive real-time data and spot patterns that might indicate potential security breaches. This proactive strategy facilitates rapid decision-making and the optimal allocation of resources for cybersecurity endeavors. Moreover, real-time monitoring empowers organizations to anticipate emerging security threats and adjust their security strategies accordingly. In essence, real-time monitoring is a crucial element in safeguarding sensitive information and upholding the integrity of identity and access management systems in today's constantly changing threat environment.

## 3. Application of Machine Learning in Identity and Access Management Systems

### 3.1. User Behavior Analysis

The application of Machine Learning (ML) algorithms in identity and access management systems is crucial for bolstering security in the digital domain. As stated by scholarly sources [10], the increasing sharing of personal data online necessitates a robust framework to guarantee privacy and security on social networks. Additionally, the integration of ML methodologies, as pointed out in scholarly discussions [11], presents a route to constructing self-organizing networks that adapt independently to emerging risks, thereby strengthening identity management mechanisms. Through investigating user behavioral trends and utilizing ML algorithms to interpret intricate network behaviors, entities can preemptively identify irregularities and potential security breaches. These findings facilitate a proactive stance in protecting vital digital assets, ultimately enhancing the integrity and resilience of identity and access management structures in the presence of sophisticated cyber threats.

### 3.2. Risk-based Authentication

In the area of identity and access management systems, the utilization of risk-based authentication as a fundamental strategy to reinforce security measures in response to the continually changing cyber threat landscape is evident. The necessity for seamless authentication procedures, while simultaneously upholding security and privacy standards, presents a considerable hurdle in heterogeneous user settings, as pointed out in [12]. This situation mandates a transition toward continuous authentication frameworks that make use of wearable and mobile gadgets. In addition, the inclusion of cloud computing in authentication protocols introduces further complexities, including issues related to security, privacy, and dependability, as indicated in [13]. Through the strategic integration of contemporary cryptographic techniques and technologies, organizations can tackle these challenges and advance the effectiveness of risk-based authentication tactics. This proactive strategy aligns with the overarching objective of harnessing big data and machine learning to strengthen identity and access management systems against potential susceptibilities and breaches.

### 3.3. Fraud Detection

In recent times, financial establishments have increasingly started using artificial intelligence (AI) and machine learning (ML) algorithms to bolster their fraud detection mechanisms. The traditional means of identifying financial fraud are typically laborious, costly, and subject to errors, particularly within the realm of large-scale data. By embracing sophisticated computational intelligence methodologies like data mining and classification algorithms, banks can enhance the efficiency and precision of fraud detection procedures. These technologies facilitate instantaneous tracking and evaluation of substantial datasets, facilitating prompt pinpointing of suspicious activities or deceitful conduct. Through AI-based fraud detection and prevention frameworks, financial institutions can alleviate hazards, safeguard client resources, and maintain the credibility of the banking domain. The assimilation of AI-infused resolutions in fraud detection not only simplifies functions but also enriches the comprehensive security and robustness of banking systems against evolving vulnerabilities.

### 3.4. Adaptive Access Control

The progress of artificial intelligence (AI) and machine learning (ML) technologies, as referenced in scholarly article [8], has had a substantial effect on the domains of adaptive access control within identity and access management systems. These cutting-edge technologies provide promising solutions for improving security measures through facilitating intelligent decision-making processes and effective parameter estimation, particularly within intricate and diverse network configurations. AI-driven algorithms, as exemplified in the context of fraud identification and prevention within the banking industry [8], can be tailored to adjust access control measures dynamically by leveraging real-time data analysis and predictive analytics. Through the utilization of ML algorithms for adaptive learning and reinforcement learning, enterprises can establish resilient adaptive access control mechanisms that not only adapt to changing security risks but also guarantee a smooth user experience while upholding security protocols. Fundamentally, the incorporation of AI and ML into adaptive access control systems symbolizes a pivotal advancement in fortifying cybersecurity frameworks and safeguarding sensitive data in modern network landscapes.

### 3.5. Continuous Authentication

The notion of Continuous Authentication serves a pivotal role within the realm of identity and access management frameworks, especially within the spheres of online evaluations and cloud security frameworks. The ground-breaking strategy illustrated in the work cited as [14] proposes a pragmatic resolution by endorsing the appending of voice excerpts to digitally sign the endeavors of a participant. This measure guarantees genuineness and wholeness in scholastic settings. This strategy tackles the pressing issue of verifying the identity of individuals partaking in internet undertakings, which is in line with the primary aim of authentication structures. Additionally, as emphasized in [15], the complexities linked to security and confidentiality in cloud amenities necessitate advanced cryptographic mechanisms to shield user information. Through the assimilation of continuous authentication techniques substantiated by contemporary cryptography, the domain of identity and access management can be strengthened against developing perils, fundamentally amplifying the comprehensive security stance of digital functions.

## 4. Challenges and Limitations of Implementing Big Data and Machine Learning in Identity and Access Management Systems

### 4.1. Data Privacy and Compliance

Within the domain of data privacy and compliance, the ever-changing landscape of managing personal data calls for novel interventions to enable individuals and alleviate power differentials. At the core of this discussion lies the notion of Personal Data Stores (PDSes), as elaborated in [16], which put forward the idea of longitudinal, decentralized, and person-centric strategies for data aggregation and maintenance. These structures not only focus on the independence of data subjects but also contest the supremacy of large-scale service providers. Moreover, the examination of privacy-enhancing technologies and organizational strategies, as deliberated in [17], highlights the significance of adhering to GDPR guidelines when dealing with data challenges in the domain of big data. Through a critical analysis of these perspectives, entities can navigate the intricacies of data privacy, ensuring compliance with stipulated rules while harnessing the capabilities of data-centric systems in the sphere of identity and access management.

### 4.2. Integration Complexity

The integration of Internet of Things (IoT) into Smart Grid Systems (SGs) causes increased intricacy, especially in the areas of security and data handling. As SGs progress to tackle challenges related to information dissemination, energy effectiveness, and dependability, embedding IoT devices is imperative for facilitating two-way energy transfer and advanced monitoring capabilities. Nonetheless, this merger also raises fresh hurdles concerning connectivity, automation, and monitoring a large number of widely dispersed devices within the grid. By concentrating on security issues surrounding IoT infrastructures, the intricacy of overseeing and safeguarding these interconnected systems escalates. To efficiently exploit the advantages of IoT in SGs without jeopardizing their credibility, an elaborate comprehension of integration intricacies and a proactive strategy for tackling associated security threats are crucial elements for ensuring the robustness of identity and access management systems in the evolving milieu of big data and machine learning technologies.

### 4.3. Scalability Issues

In the contemporary landscape of extensive data and computational intelligence, organizations encounter a profound hurdle concerning the expansion of identity and access management (IAM) frameworks. Managing the escalating quantities of users, gadgets, and information resourcefully, while upholding security and performance standards, emerges as a pivotal apprehension. The complexity of IAM structures, the fluctuating demands for user access, and the swift enlargement of digital environments contribute to potential scalability impediments. Scholarly inquiry conducted by the Vienna University of Economics and Business and the Regional Centre of Expertise on Education for Sustainable Development underscores the vitality of confronting scalability challenges in IAM frameworks [18]. The incorporation of pioneering methodologies that exploit big data analytics and machine learning unveils profound insights into user conduct, fortifies access regulations, and bolsters a sturdier and scalable IAM edifice. By amalgamating cutting-edge technologies with industry best practices, entities can adeptly transcend the scalability predicaments ingrained in contemporary IAM structures, thereby guaranteeing the security and efficacy of access management procedures.

### 4.4. Model Interpretability

When contemplating the utilization of machine learning models to fortify Identity and Access Management Systems, a pivotal element necessitating meticulous examination is the interpretability of the model. The burgeoning domain of deep learning within recommender systems, as emphasized in a scholarly work [19], underscores the significance of comprehending the decision-making mechanisms of these intricate models within the realm of security. Furthermore, a study [20] delves into the amalgamation of Artificial Intelligence and Machine Learning in digital forensics, stressing the importance of clarity in algorithmic decision-making procedures. In the sphere of identity and access management, guaranteeing the interpretability of machine learning models is essential for audit trail purposes, conformity with regulations, and fostering confidence among system users. By exploring methodologies to enrich model interpretability, for instance, through feature representation and elucidation techniques post-model development, entities can reinforce the security posture of their systems while concurrently enhancing liability and facilitating judicious decision-making procedures.

### 4.5. Security Risks

The reliance of organizations on cloud computing for storage and processing is on the rise, leading to an increased need for the evaluation and management of security risks. Cloud computing offers cost benefits but also brings challenges in upholding data privacy and dependability. The notion of cloud computing, coupled with the surge in interconnected industrial control systems and the incorporation of IoT principles, is eroding traditional isolation techniques and ushering in enhanced connectivity, sparking concerns regarding cybersecurity and safety [21]. These transformations underscore the urgent requirement for robust security protocols in response to the changing technological environments. Safeguarding identity and access management systems demands a thorough evaluation of potential vulnerabilities stemming from these emerging patterns. Organizations can enhance their defensive mechanisms against cyber threats and uphold the integrity of their data assets in the digital era by tackling these security risks through advanced cryptographic tools and proactive strategies.

## 5. Conclusion

This study underscores the growing significance of cooperative frameworks, advanced technologies, and ethical considerations in shaping the future of identity and access management (IAM) systems. Evidence from Spanish machine-tool cooperatives illustrates how inter-cooperation strategies, including shared R&D initiatives, collaborative sales channels, and knowledge exchange, facilitate innovation and global competitiveness while mitigating opportunism. The Co-Curate North East project further demonstrates the potential of socially driven digital platforms in fostering identity formation and community-based learning, offering a template for participatory and decentralized knowledge curation.

Simultaneously, the integration of emerging technologies such as cyborg systems, health-related IoT (H-IoT) devices, and AI-driven automation introduces new capabilities and challenges. As neural interfaces and bio-integrated tools begin to merge with service delivery models, the concept of 'melded' human-machine personnel may fundamentally transform how organizations address complex identity governance scenarios. These advances demand that ethical and regulatory considerations—particularly data privacy and system transparency—remain central in both design and implementation.

Looking ahead, future research must explore scalable, secure, and interpretable IAM systems that align with the dynamics of big data, machine learning, and decentralized infrastructures. Technologies like blockchain and mobile edge computing present promising avenues for secure, real-time data management, especially in sensitive sectors like healthcare. However, success will depend on addressing key technical challenges such as minimizing communication overhead, optimizing resource usage, and ensuring algorithmic fairness.

From a practical standpoint, cloud-centric penetration testing remains essential to safeguarding IAM systems, especially given the evolving complexity of cloud environments. Incorporating best practices and secure deployment architectures, such as BradStack, is critical to verifying the robustness of IAM infrastructures across platforms like AWS, Azure, and GCP.

Ultimately, while big data and AI offer unprecedented capabilities for anomaly detection and adaptive access control, their deployment must be guided by a commitment to transparency, privacy, and user empowerment. Organizations must invest not only in the technologies themselves but also in the human expertise needed to manage them responsibly. As IAM continues to evolve, interdisciplinary research and practice will play a pivotal role in ensuring secure, ethical, and resilient identity ecosystems.

## References

[1] N. Ghadge, "Enhancing threat detection in Identity and Access Management (IAM) systems," International Journal of Science and Research Archive, vol. 11, no. 2, pp. 2050–2057, 2024, doi: https://doi.org/10.30574/ijsra.2024.11.2.0761.

[2] Y. Saleem, N. Crespi, M. H. Rehmani, and R. Copeland, "Internet of Things-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions," IEEE Access, vol. 7, pp. 62962–63003, 2019, doi: https://doi.org/10.1109/access.2019.2913984.

[3] C. Anglano, M. Canonico, and M. Guazzone, "Forensic analysis of Telegram Messenger on Android smartphones," Digital Investigation, vol. 23, pp. 31–49, Dec. 2017, doi: https://doi.org/10.1016/j.diin.2017.09.002.

[4] Vijay Gadepally and J. Kepner, "Big data dimensional analysis," arXiv (Cornell University), pp. 1–6, Sep. 2014, doi: https://doi.org/10.1109/hpec.2014.7040944.

[5] Z. Md. Fadlullah et al., "State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow's Intelligent Network Traffic Control Systems," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2432–2455, 2017, doi: https://doi.org/10.1109/comst.2017.2707140.

[6] Y. Sun, M. Peng, Y. Zhou, Y. Huang, and S. Mao, "Application of Machine Learning in Wireless Networks: Key Techniques and Open Issues," IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3072–3108, 2019, doi: https://doi.org/10.1109/comst.2019.2924243.

[7] N Ghadge, "Digital Identity in the Age of Cybersecurity: Challenges and Solutions," Global Journal of Computer Science and Technology, pp. 1–9, May 2023, doi: https://doi.org/10.34257/ljrcstvol24is1pg1.

[8] M. M. Alhaddad, "Artificial Intelligence in Banking Industry: A Review on Fraud Detection, Credit Management, and Document Processing," ResearchBerg Review of Science and Technology, vol. 2, no. 3, pp. 25–46, Nov. 2018, Available: https://researchberg.com/index.php/rrst/article/view/37

[9] M. Hu, "Algorithmic Jim Crow," FLASH: The Fordham Law Archive of Scholarship and History, 2017. https://ir.lawnet.fordham.edu/flr/vol86/iss2/13/ (accessed Apr. 17, 2025).

[10] J. Moura and C. Serrao, Security and Privacy Issues of Big Data. 2015. Available: https://arxiv.org/abs/1601.06206

[11] P. V. Klaine, M. A. Imran, O. Onireti, and R. D. Souza, "A Survey of Machine Learning Techniques Applied to Self-Organizing Cellular Networks," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2392–2431, 2017, doi: https://doi.org/10.1109/comst.2017.2727878.

[12] R. F. Olanrewaju, B. U. I. Khan, M. A. Morshidi, F. Anwar, and M. L. B. M. Kiah, "A Frictionless and Secure User Authentication in Web-Based Premium Applications," IEEE Access, vol. 9, pp. 129240–129255, 2021, doi: https://doi.org/10.1109/access.2021.3110310.

[13] Mehmet Sabır Kiraz, Muhammed Ali Bingöl, Süleyman Kardaş, and Fatih Birinci, "Anonymous RFID Authentication for Cloud Services," International Journal of Information Security Science, vol. 1, no. 2, pp. 32–42, Jul. 2012.

[14] S. Y. Kung, M. W. Mak, and S. H. Lin, Biometric Authentication: A Machine Learning Approach. 2004.

[15] M. S. Kiraz, "A comprehensive meta-analysis of cryptographic security mechanisms for cloud computing," Journal of Ambient Intelligence and Humanized Computing, vol. 7, no. 5, pp. 731–760, Jun. 2016, doi: https://doi.org/10.1007/s12652-016-0385-0.

[16] K. U. Fallatah, M. Barhamgi, and C. Perera, "Personal Data Stores (PDS): A Review," Sensors, vol. 23, no. 3, p. 1477, Jan. 2023, doi: https://doi.org/10.3390/s23031477.

[17] O. G. Yalcin, "GDPR Compliant Data Processing and Privacy Preserving Technologies: A Literature Review on Notable Horizon 2020 Projects," Advances in Intelligent Systems and Computing, pp. 166–177, Oct. 2021, doi: https://doi.org/10.1007/978-3-030-87687-6_17.

[18] Shermin Voshmgir, M. Wildenberg, C. Rammel, and T. Novakovic, "Sustainable Development Report: Blockchain, the Web3 & the SDGs," Dec. 2019.

[19] S. Zhang, L. Yao, A. Sun, and Y. Tay, "Deep Learning Based Recommender System," ACM Computing Surveys, vol. 52, no. 1, pp. 1–38, Feb. 2019, doi: https://doi.org/10.1145/3285029.

[20] D. Dunsin, M. C. Ghanem, K. Ouazzane, and V. Vassilev, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response," Forensic Science International: Digital Investigation, vol. 48, no. 301675, p. 301675, Mar. 2024, doi: https://doi.org/10.1016/j.fsidi.2023.301675.

[21] C. Johnson, "Securing the Participation of Safety-Critical SCADA Systems in the Industrial Internet of Things," 2016. Accessed: Apr. 17, 2025. [Online]. Available: https://eprints.gla.ac.uk/130828/1/130828.pdf