International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Enhancing Healthcare Security with AI-Driven Identity and Access Management

Mahendra Krishnapatnam

Cybersecurity Professional, Premier Service Provider Organization, Chicago, Illinois, United States

Abstract: ***The healthcare industry faces critical challenges in Identity and Access Management (IAM), requiring robust security while ensuring regulatory compliance. Traditional IAM approaches often fail to meet evolving threats, necessitating AI-driven solutions for enhanced security and efficiency. This study explores the role of Artificial Intelligence (AI) in IAM, highlighting AI-driven authentication, fraud prevention, and risk-based access control. Using machine learning and behavioral analytics, AI automates identity verification, enhances compliance with HIPAA and GDPR, and mitigates unauthorized access risks. Through real-world case studies, this paper demonstrates how AI-based IAM strengthens security, reduces administrative overhead, and ensures seamless access control in healthcare.***

Keywords: AI-Driven IAM, Cybersecurity in Healthcare, Risk-Based Authentication, Compliance, Identity Verification.

1. Problem Statement

The healthcare sector is increasingly vulnerable to cybersecurity threats, identity fraud, and stringent regulatory requirements, necessitating advancements in IAM solutions. Legacy IAM frameworks often lack scalability, automation, and adaptive security measures, leading to vulnerabilities in protecting sensitive data and ensuring seamless access for patient and healthcare data.

Key issues include:

- Identity Fraud & Unauthorized Access: The rise of cyber threats, including phishing and credential theft, compromises patient records, leading to privacy breaches and compliance violations.
- Operational Inefficiencies: Manual identity verification and access management processes create delays in critical healthcare operations, impacting productivity.
- Regulatory Compliance Challenges: Meeting stringent regulations such as HIPAA, HITECH, and GDPR demands advanced identity governance, continuous monitoring, and risk-based access controls.
- Lack of Adaptive Security Measures: Traditional authentication mechanisms, such as passwords, fail to provide context-aware and AI-driven security, leaving systems vulnerable to insider threats and evolving attack vectors.

To address these problems, this study explores the role of Artificial Intelligence (AI) in transforming IAM security for healthcare. Through real-time continuous risk-based authentication and biometric verification, AI-driven IAM solutions not only mitigates the cyber threats, but also streamlines access control and regulatory compliance. The proposed framework leverages ML to automate identity verification, reducing manual inefficiencies while safeguarding sensitive healthcare data.

This study contributes to the evolving field of healthcare security by providing a structured AI-driven IAM framework that balances security, compliance, and operational efficiency. It aims to help healthcare organizations safeguard sensitive patient data while streamlining identity verification and access control.

2. Solution

To address the critical challenges in Identity and Access Management (IAM) within the healthcare industry, Artificial Intelligence (AI)-driven IAM solutions provide a transformative approach that enhances security, operational efficiency, and regulatory compliance.

The proposed solutions include:

1) Multi-Factor Authentication

- Before enabling an AI-driven framework, it is essential to establish a strong foundation by requiring users to register for Multi-Factor Authentication (MFA). Organizations should prioritize only highly secure MFA methods, such as push notifications and biometrics, to enhance security. Additionally, an MFA framework—guided by policies or rules—should be designed to enforce MFA authentication, especially for applications accessed from outside the company network. IAM administrators must enforce that highly vulnerable identity validation methods using SMS OTPs or Email OTPs (which are prone to Man-In-the-Middle attacks) must be forbidden for user MFA registration.

2) AI-Powered Identity Verification & Fraud Prevention

- Implement ML-driven identity verification to detect anomalies and prevent identity fraud using Random Forest, Neural networks models.
  NOTE: There are few products in the market that can be evaluated to ensure that it meets customer requirements for AI/ML driven framework.
- Use biometric authentication (facial recognition, voice, fingerprint scanning) to strengthen identity validation and eliminate reliance on passwords. An additional secured method Windows Hello for business is also widely accepted which uses Biometric authentication for device login and/or user login.

3) Risk-Based & Adaptive Authentication

- Deploy AI-driven risk-based authentication (RBA) that dynamically adjusts security levels based on real-time user behavior, device intelligence, and geolocation data. The risk-based authentication would be available in two modes, learning and preventive mode. To collect

profiling data, it should be enabled in learning mode where it collects all fingerprinting data for all transactions for couple of weeks depending upon the data collected. Once the data collected is deemed sufficient, IAM administrators should analyze and enable it in Preventive mode using rules/policies appropriately. Often, it may be repetitive process of learning and preventive modes for application(s) depending upon volume of user access.

- Based on the device fingerprinting data such as IP address, location, timestamp, browser type, device OS etc., with time the system would accumulate profiling data.
- Enforce adaptive multi-factor authentication (MFA) and passwordless authentication, reducing friction while maintaining security. Passwordless authentication leverages MFA as broker to mediate the authenticate with MFA provider and the client.
- Passwordless authentication enhances security by eliminating several vulnerabilities such as phishing attacks, credential-based attacks, brute-force attacks, and adversary-in-the-middle attacks.

4) Zero-Trust Security Framework

- Implement a Zero-Trust model, ensuring continuous identity verification and least-privilege access based on contextual risk assessment. This involves using granting access based on job roles using RBAC model and providing access to sensitive resources only as needed using JIT model. Also, access is granted based on real-time user context attributes such as location, device, security posture in a time-bound manner.
- Utilize AI-driven behavioral analytics to detect anomalies and insider threats proactively. With time, once AI records the patters of user activity including login time, frequency, location and applications/system accessed, file accessed, keystore dynamics, it established a behavioral baseline. Then, this baseline data is used for future access to detect threats. This data certainly varies between patient and healthcare, thereby establishing separate behavioral patterns and anomalies detection.

5) Automated Identity Lifecycle Management

- Integrate AI-based automation for role-based access control (RBAC) and attribute-based access control (ABAC) to assign and revoke access dynamically. A very common example is assigning access to an application/system based on job code. Once the user is appraised or relegated, access to the system is automatically revoked as the job code changes.
- Enhance privileged access management (PAM) using AI to monitor and control high-risk user activities. While privileged accounts are the primary targets for bad guys as they have access to critical systems, AI can be used for continuous monitoring using login frequency, time and location of the access along with commands executed in sessions, file or systems access and tools used.

6) Regulatory Compliance & Auditing

- Employ AI-driven compliance monitoring to ensure adherence to HIPAA, GDPR, and other healthcare regulations. HIPPA mandates privacy, security and breach notification rules for PHI, AI enhances HIPAA by tracking unauthorized access to patient data, detecting unauthorized file transfers, monitoring emails for sending PHI data etc., GDPR requires data protection, consent management and breach notification for EU users data. AI can help address GDPR compliance by speeding up processing requests from patients or physicians who want access to or deletion of their data, monitoring data transfers, and detecting unauthorized data sharing. It is essential to implement end to end encryption and privacy preserving AI methods (differential privacy and federated learning) while analyzing sensitive healthcare data.
- Automate audit logging, reporting, and security incident detection for proactive risk management. AI collects logs from various sources such as user authentication logs, file access logs, endpoint logs, PAM logs etc., for detection and reporting. One of the commonly observed detections is when abnormal user activity occurs or when a compromised account is used to access sensitive systems.

3. Roadmap for Adopting AI framework

Implementing AI-based IAM framework in healthcare requires strategic approach to ensure compliance, efficiency and security are well-balanced. High level roadmap as shown below outlines every phase, action defined, possible outcomes and various stakeholders involved.

Phase	Key Actions	Outcome	Stakeholders Involved
Assessment & Planning	1) Define IAM goals 2) Conduct risk assessment 3) Document use cases	IAM aligned with security, compliance & operational goals	IAM Architect IAM Manager Business Analyst
Technology Selection/Evaluation	1) Evaluate AI IAM solution 2) Choose AI IAM Solution 3) Implement AI IAM Solution	AI-powered authentication & access control implemented	AI vendors IAM Architect IAM Manager Legal/Compliance Team
Deployment & Integration	1) Integrate IAM target apps 2) Integrate workforce applications/patient/hospital systems 3) Implement AI access controls	Secure, automated identity verification & access management,	IAM Architect IAM/AI Engineers IAM Manager
Security Monitoring & Compliance	1) Deploy AI threat detection 2) Automate compliance audits	Real-time security monitoring & regulatory compliance	IAM/AI Engineers IAM Manager
Training, Optimization & Scaling	Staff training, AI IAM optimization, expansion across networks	Fully optimized AI IAM with long-term scalability	IAM/AI Engineers IAM Manager

4. Challenges

While AI based IAM framework offers great benefits to healthcare security, ease of access, compliance; their implementation comes with various challenges as outlined below.

1) Privacy and Data Exposure

Healthcare organizations handle sensitive patient data, and AI-driven IAM systems must comply with regulations like HIPAA, GDPR, and HITECH.

Appropriate privacy preserving AI methods must be implemented such as federated learning, to minimize data exposure. Often, the data could be hosted on Cloud, hence take appropriate measures to ensure that end to end encryption is used using trusted certificate authority.

Regulatory Compliance – AI systems must align with strict regulations, and failure to do so can lead to legal consequences and financial penalties.

2) Legacy Healthcare Systems limiting adoption of AI frameworks

Many healthcare organizations still operate on legacy IT infrastructure, making AI integration difficult.

Outdated IAM Systems – Older systems may not support AI-driven authentication methods such as behavioral biometrics. Gradually modernize IAM infrastructure and adapting hybrid IAM solution that support both traditional and AI-driven methods. This might also involve working with legacy application teams to upgrade the application to use open standards.

3) Cybersecurity Threats and AI Exploitation

While AI can improve IAM security in healthcare, it could be still vulnerable to AI powered cyberattacks where hackers may use adversarial AI techniques to manipulate authentication models and bypass security measures and perform identity spoofing using deepfake videos to trick biometric authentication platform.

4) High Implementation and Maintenance Costs

AI-driven IAM systems require significant investment in technology, infrastructure, and expertise and it could be costing time. This could require purchasing AI products that meets these requirements, evaluation of the product and rollout eventually. This also involves hiring high-tech AI professional or provide deep-dive training to security administrators.

5) User Resistance and Adoption

AI-driven IAM introduces new authentication methods, which may face resistance from healthcare employees and stakeholders. This is very commonly noticed that involves delayed process by seeking approvals from various stakeholders such as Architecture Review boards, Legal & Compliance team. Help desk team could also be involved as it this could change the overall user experience. There could be resistance towards using modern technology such as hardware token based passwordless authentication or additional MFA devices. If the organization has already rolled out MFA using vulnerable authentication methods, then it could be daunting job to re-enforce MFA enrollment with highly secured methods.

6) Scalability & Performance

As healthcare systems expand, IAM solutions must be able to scale proportionally.

Increased healthcare data volume could cause AI systems to process massive amounts of user data, which can strain resources. On the other hand, adding AI-driven frameworks might cause slowness to application access or could result in extra steps for authentication / authorization flow.

5. Conclusion

AI is fundamentally transforming Identity and Access Management (IAM) in healthcare, strengthening security, improving operational efficiency, and ensuring regulatory compliance in an industry where safeguarding sensitive patient data is critical. By leveraging AI-driven authentication, behavioral biometrics, and machine learning-based anomaly detection, healthcare organizations can proactively reduce unauthorized access risks, streamline identity verification, and maintain compliance with regulations such as HIPAA and GDPR.

Despite its advantages, AI-driven IAM presents challenges, including privacy concerns, potential bias in AI models, cybersecurity threats, high implementation costs, and the complexity of integrating with legacy systems. To address these challenges, organizations must adopt a balanced approach, combining explainable AI, hybrid IAM architectures, advanced threat detection, and user-friendly authentication mechanisms. Ensuring security without disrupting healthcare workflows requires continuous monitoring and human oversight alongside AI-driven automation.

As AI technology evolves, its role in IAM will become even more pivotal. Future research should focus on integrating AI with decentralized identity frameworks, federated learning models, and privacy-preserving techniques such as zero-knowledge proofs and homomorphic encryption—to enhance security while maintaining a seamless user experience. By strategically adopting AI-powered IAM, healthcare organizations can establish a resilient, future-proof security model that ensures the right individuals access the right information at the right time without compromising security or efficiency.

References

[1] Identity Management Institute. (n.d.). *Adaptive authentication and behavior analytics*. Retrieved February 13, 2025, from https://identitymanagementinstitute.org/adaptive-authentication-and-behavior-analytics/

[2] ScienceDirect. (2023). *The effects of behavioral analytics in identity management*. *Elsevier*. Retrieved February 13, 2025, from https://www.sciencedirect.com/science/article/abs/pii/S0952197623014021

[3] Feedzai. (2023, September 19). *Behavioral biometrics: Next-generation fraud prevention*. Retrieved February 13, 2025, from

https://www.feedzai.com/blog/behavioral-biometrics-next-generation-fraud-prevention/

[4] Kapron, Z. (2025, January 27). *Beyond the swipe: How artificial intelligence is redefining biometrics*. *Forbes*. Retrieved February 13, 2025, from https://www.forbes.com/sites/zennonkapron/2025/01/27/beyond-the-swipe-how-artificial-intelligence-is-redefining-biometrics/

[5] Sardine. (2023, July 14). *How can behavioral biometrics prevent fraud?* Retrieved February 13, 2025, from https://www.sardine.ai/blog/how-can-behavioral-biometrics-prevent-fraud

[6] Infisign. (2023, November 10). *AI in identity and access management*. Retrieved February 13, 2025, from https://www.infisign.ai/blog/ai-in-identity-and-access-management

[7] CDW. (2023, August 12). *Navigating identity & access management in the era of AI*. Retrieved February 13, 2025, from https://www.cdw.com/content/cdw/en/articles/security/navigating-identity-access-management-in-era-ai.html

[8] Advantage Technologies. (2023, December 5). *Using AI to enhance IAM security and user experience*. Retrieved February 13, 2025, from https://www.advantage.tech/using-ai-to-enhance-iam-security-and-user-experience/

[9] Identity Management Institute. (n.d.). *AI-driven identity governance and administration*. Retrieved February 13, 2025, from https://identitymanagementinstitute.org/ai-driven-identity-governance-and-administration/

[10] Online Scientific Research. (2024). *Revolutionizing role-based access control: The impact of AI and ML in identity and access management*. Retrieved February 13, 2025, from https://www.onlinescientificresearch.com/articles/revolutionizing-rolebased-access-control-the-impact-of-ai-and-machine-learning-in-identity-and-access-management.html

[11] World Journal of Advanced Research and Reviews. (2024). *AI in identity and access management: Trends and challenges*. *WJARR*, 7(1), 45-53. Retrieved February 13, 2025, from https://wjarr.com/sites/default/files/WJARR-2024-3501.pdf