National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

HEALTHCARE SECURITY & Smart Authentication

Contributors

Mehwash Weqar

Department of Electrical Engineering,
Jamia Millia Islamia. New Delhi-110025,
India.

mehwash.weqar@gmail.com

Shabana Mehfuz

Department of Electrical Engineering,
Jamia Millia Islamia. New Delhi-110025,
India.

smehfuz@jmi.ac.in

Table of CONTENTS

1	Introduction	4
2.	Identity Acess Management in IoHT Networks	8
3.	Challenges and Solutions	14
4.	Conclusion and Future Road map	17

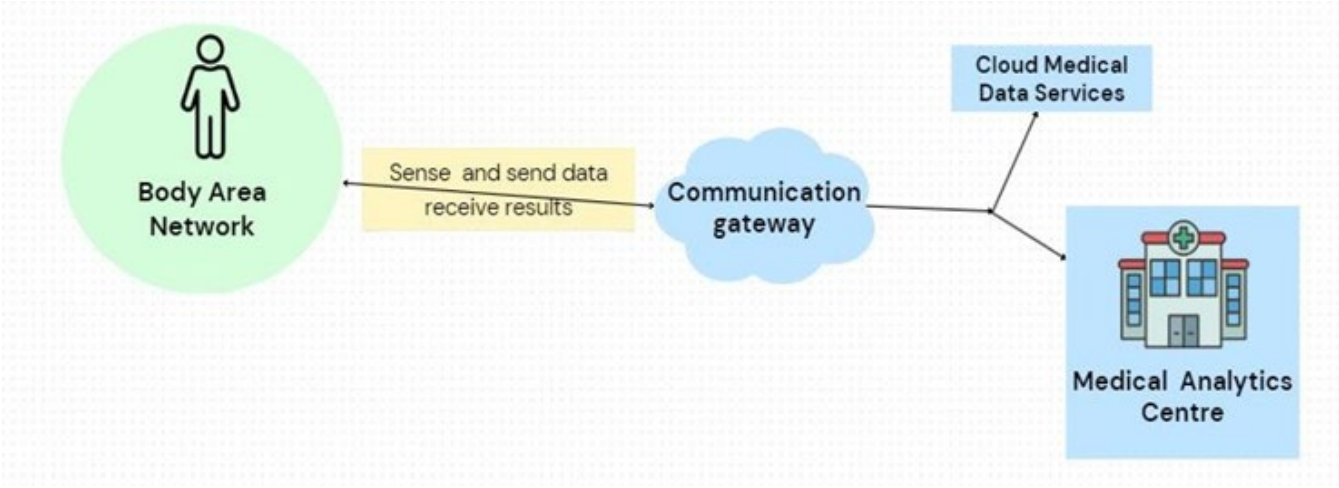
1 Introduction

A widely used technological innovation called the Internet of Things describes a cyber physical communication network that integrates, wireless sensor network (WSN), and M2M (machine-to- machine) interaction which makes it possible for any "object" to communicate messages, thus linking all of the intelligent objects and things globally.

The Internet of Things (IoT) framework is a specific area of technology that encourages innovation across a number of industries. IoT is a key enabler of improved quality of life in different industries, especially healthcare. An immense variety of healthcare applications, including online medical care, intelligent medical treatment, on location surveillance of patients, remote recommendations, residential care, tracking behavior modifications, compliance with treatments, hospital facility administration, and more, can be developed and implemented with the help of IoT. These applications which can be accessed via Internet have resulted in remarkable progress in patient monitoring, assessment, medication, and other areas of the health-care industry.

IoHT (Internet of Healthcare Things) system enables healthcare professionals to identify ailments with greater speed and precision as they have continual tracking of patients, which provides them with real-time healthcare data. Figure 1 shows a possible configuration for the Internet of Healthcare Things network. Sensors worn by people and carry-around medical devices attached to the body of the person are used to gather and document the patient's health related parameters. A gateway on the network transmits data from a variety of sensors and devices to the target health care system. The firms offering these services might be the health sector servers or any kind of medical information analysis center, where the collected data is subsequently assessed and utilized to keep health records.

Figure 1. Internet of Healthcare Things Network.



Thus, IoT has considerable amount of efficacy to improve healthcare by reducing medical expenses, enhancing therapeutic outcomes, enhancing user experience and hence raising the standard of life.

1.2 Types of cyberthreats present in Health- care domain

The vulnerability of IoT devices increases with the exponential increase in their number. By connecting to the system, an intruder can get access, take advantage of security flaws, and take

over the network as a whole. These issues are critical for potential applications in the health care system. Among the main challenges affecting the IoHT network are:

1.2.1 Data Breaches: It is the unauthorized access of personal health information (PHI). Stealing of confidential patient information from devices with insufficient encryption or inadequate safety features.

1.2.2 Ransomware: Healthcare data is encrypted by attackers, who then demand cash to release it, which may negatively affect patient care and result in disruptions of services.

1.2.3 Device Vulnerabilities: Some medical devices, such as pumps for insulin, pacemakers, and health monitoring platforms, may not have the necessary security features because of obsolete software or a lack of resources. Attackers may take advantage of these flaws to alter device operations or gain entrance to a global network.

1.2.4 Denial of Service (DoS): Attackers have the ability to overload IoHT networks and linked devices with the flow of traffic, which can lead to breakdowns or outright device failures. This can be devastating in cases where life is at risk.

1.2.5 Man-in-the-Middle (MitM): Communications interception: Data transferred between linked healthcare equipment and systems can be intercepted or modified by attackers. This can result in revised diagnosis, erroneous treatment regimens, or poor examination of patients.

1.2.6 Malware: IoHT device infection caused by malware: Malware can propagate throughout an IoHT network, infecting devices and networks in order capture information, interfere with processes, or allow unwanted access. Malware outbreaks may propagate quickly across networks due to the vast number of devices linked together.

1.2.7 **Phishing:** Healthcare staff fraud: Social engineering tactics and scam emails are frequently used to fool healthcare personnel into downloading malware or disclosing login information. This can lead to illegal access to health care organizations and highly confidential data.

1.2.8 **Weak Authentication:** Inadequate access for user management: A lot of IoHT platforms and gadgets utilize preset or insecure passwords, that can be conveniently cracked. Attackers can obtain unauthorized access to vital medical equipment and patient data due to inadequate access restrictions.

1.2.9 **Outdated Systems:** shortcomings in obsolete or outdated systems: A lot of healthcare organizations employ these systems, which do not get updates on a regular basis and are therefore susceptible to known vulnerabilities. IoHT devices with unpatched firmware and software can provide an entry point for hackers.

These frequent attacks highlight the necessity of strong security protocols, such as encryption, frequent upgrades, strong authentication, and ongoing monitoring, in order to protect IoHT networks.

1.3 Importance of cybersecurity in Internet of Healthcare Things (IoHT) Network.

The confidential character of healthcare data and the important function that interconnected equipment play in dealing with patients, lead to the essential requirement of cybersecurity in the Internet of Healthcare Things (IoHT) network. One way to sum up the significance of cybersecurity in IoHT is as follows:

1.3.1 **Safeguarding Private Patient Information:** Large volumes of sensitive personal health information (PHI), which needs to be protected to preserve patient privacy, are collected and transmitted by IoHT devices. Cybersecurity guarantees that this data is safe, secure, and unreadable by outsiders, preventing fraud, identity theft, and improper use of medical data.

1.3.2 **Preserving Patients Security:** Numerous IoHT components, have a direct effect on patients' health. These technologies are susceptible to cyberattacks that could impair their functionality or result in incorrect diagnoses or treatments, endangering human life. Cybersecurity assures ensuring that gadgets are not tampered with and operate as intended.

1.3.3 Sustaining Operational Availability: For everyday operations, hospitals and healthcare professionals depend on networked equipment and systems. Cyberattacks that cause service outages, such as ransomware or denial of service (DoS), could halt medical care and remedies. Strong cybersecurity safeguards contribute to the ongoing provision of medical treatments.

1.3.4 **Avoiding Monetary Risks:** Healthcare companies may suffer large financial losses as a result of cyberattacks, which can include making ransom payments, being fined, and experiencing disruptions in operation. Robust cybersecurity serves to lessen the likelihood of attacks and their possible financial consequences.

1.3.5 **Developing Patient Confidence:** Patients anticipate safety and sensitive data protection from their healthcare providers. Ensuring patients that their health and information are secure is one way that robust cybersecurity policies foster patient trust.

1.3.6 **Reducing Internal Possible Risks:** Internal threats, whether deliberate or unintentional, can occur in healthcare environments. Cybersecurity measures like monitoring and access control help stop insiders from gaining unauthorized access to highly confidential data or vital systems.

1.3.7 **Protection against New Security concerns:** As the use of IoHT increases, so do the potential for cyberthreats such as ransomware, sophisticated malware, and personal information thefts. Sustained investment on cybersecurity is necessary to guarantee system resilience and shield IoHT networks from ever changing threats.

1.3.8 Growing Complexity of Cyberthreats

a) Advanced Persistent Threats (APTs): These protracted, focused assaults aim to penetrate healthcare networks covertly over an extended length of time. They have the ability to hack into vital IoHT equipment or steal patient data.

b) Zero-Day Exploits: Before updates are released, hackers are more frequently taking advantage of undiscovered flaws in IoT or health care equipment.

1.3.9 Vulnerabilities in Conventional Password-Based Authentication

a) Password Fatigue and Reuse: Because a lot of medical professionals have to use a variety of programs and machines, they frequently end up with ineffective, repeated, or lost passwords that are very vulnerable to spoofing and other attack vectors.

b) Credential Theft: By using brute-force attacks, phishing schemes, or compromised password databases, cybercriminals are becoming more and more capable at taking advantage of user credentials.

Therefore, in the context of IoHT, cybersecurity is essential for safeguarding patient data, maintaining service stability, ensuring equipment dependability, adhering to legal requirements, and shielding healthcare institutions from damage to their finances and credibility.

The current state of advanced threats, particularly in relation to the Internet of Healthcare Things (IoHT), is primarily caused by the frequency and sophistication of cyberattacks that target healthcare systems, gadgets, and confidential information.

With the healthcare sector becoming increasingly computerized, linked, and based on information, conventional authentication methods (such passwords) are not anymore adequate to tackle current, technologically sophisticated threats.

1.4 Smart authentication for IoHT network

Smart authentication pertains to sophisticated, flexible, and safe techniques for confirming user identities and enabling access to linked medical equipment, networks, and private information concerning patients on Internet of Healthcare Things (IoHT) networks. These techniques of authentication surpass the use of standard passwords.

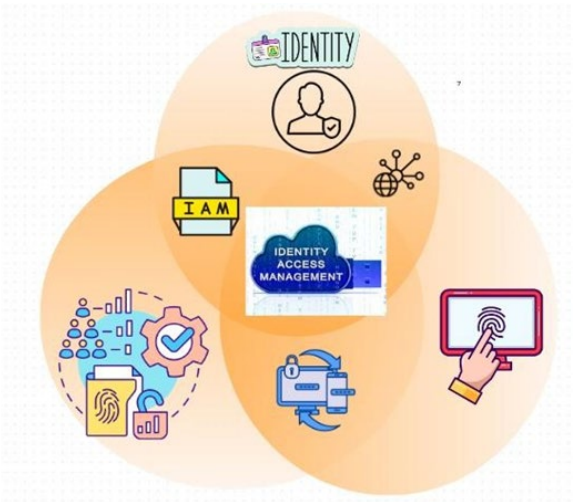
Smart authentication aims to minimize risks like data theft, device tampering or illegal access while offering an uninterrupted however extremely reliable interaction. It does this by guaranteeing that only those with authorization can connect to and communicate with IoHT equipment and networks.

2

Identity Access Management in IoHT Networks

Authentication, Authorization, and Accounting, or Identity and Access Management (IAM) as it is also referred to, is a crucial component of a company's information security. It entails controlling the permissions that are granted for users and other elements to a variety of internal assets and services. Figure 2 shows the various sectors of Identity Access Management.

Figure 2 : IAM sectors



2.1 Understanding IAM types & tools

A set of guidelines, tools, and technologies known as Identity and Access Management (IAM) makes certain that the right people or objects are given permission to utilize the information and assets within a corporation. Regulating the accessibility of networks, platforms, and information as well as maintaining identities (user or device), are all part of it. IAM helps to satisfy compliance standards, improves user satisfaction, and assures security.

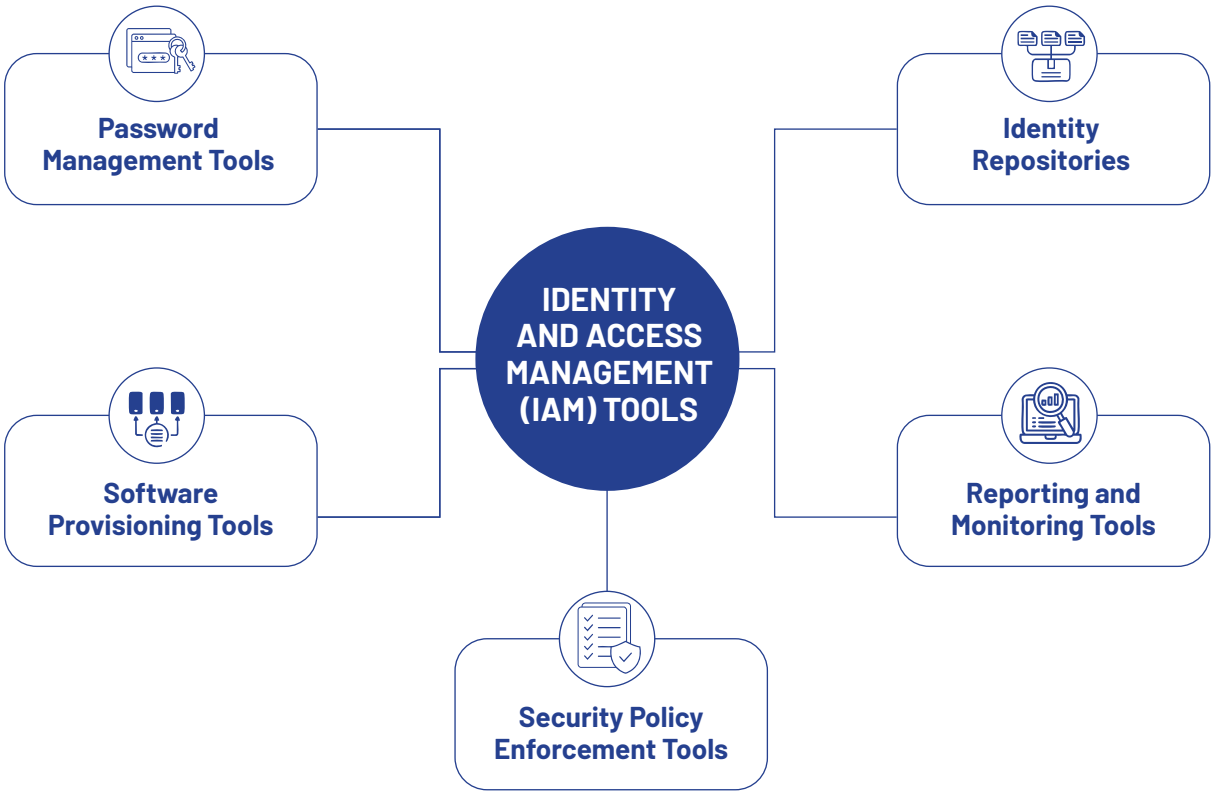
Identity management, which covers the development, upkeep, and administration electronic identifiers for individuals, equipment, and other objects within the framework of an organization, is one of the essential elements of identity and access management (IAM). In order to confirm users' identities and make sure they have the proper access permissions to the assets and services they require; this involves procedures like registration, authentication, and authorization.

Access control and monitoring of users' and other entities' access to the assets and networks inside a firm is a key component of Identity and Access Management (IAM). In order to restrict who is allowed to utilize what assets and networks along with which conditions this may involve putting establishing controls on accessibility, which include guidelines and approvals.

IAM tools might differ according to their unique scenarios and functionality. A variety of technologies and tools are often included in IAM systems. The primary IAM tool categories given in figure 3 are:

1. **Password Management Tools:** These enable you to quickly keep track of all of your passwords instead of getting to remember them all.
2. **Software Provisioning Tools:** These are tools that facilitate the management of user data between different software applications and platforms.
3. **Security Policy Enforcement Tools:** These programs make sure that inappropriate activity is promptly detected, track entry in instantaneously, and successfully implement company rules and regulations.
4. **Reporting and Monitoring Tools:** These tools keep an eye on applications with authorization and identities that could be at vulnerable.
5. **Identity Repositories:** All of the data about individuals and groups is kept in identity repositories.

Figure 3: Different Identity and Access Management (IAM) Tools, By Use-Cases



2.2 IAM in Healthcare scenario

When considering Internet of Healthcare Things (IoHT) networks, Identity and Access Management (IAM) refers to the set of guidelines, tools, and technological advancements that guarantee only authorized individuals and devices have access to IoHT devices, healthcare systems, and confidential medical data. IAM approaches are essential to safeguarding accessibility to the expanding cyberspace of healthcare companies, as they depend more and more on linked health care equipment and the IoHT network.

The workforce must receive tutorials on necessary instruments and be assisted in becoming capable in handling patient medical records and confidential information. The training of staff members is one of the most important elements of healthcare management.

Healthcare Identity and Access Management (IAM) has become a popular solution for ensuring that regular business procedures don't compromise privacy or confidentiality of information. IAM has been modified by hospital administrators to guarantee restricted authorized exposure to various documents, health care records, organizational information, and information pertaining to patients.

2.3 Current landscape of IAM in IoHT networks

The fast growth of interconnected healthcare equipment, growing risks associated with cybersecurity, and the requirement for regulatory compliance are shaping the Identity and Access Management (IAM) landscape in Internet of Healthcare Things (IoHT) networks. Important ideas consist of:

2.3.1 Expanding field of device integration: Monitoring gadget and user credentials across IoHT infrastructure.

2.3.2 Authentication and Authorization Advancements:

a) **Multi-Factor Authentication (MFA):** As biometrics and identifiers become more commonplace, MFA is crucial for ensuring safe access to medical data and systems.

b) **Threat-Based Access:** Dynamic mechanisms for authentication automatically modify security requirements by evaluating risk in response to the actions of users, position, and equipment category.

c) **Certificate-Based Authentication:** To securely communicate within healthcare systems, IoHT devices frequently need to use certificate-based techniques.

2.3.3 Compliance: Maintaining adherence to regulations (such as HIPAA and GDPR) by implementing stringent access restrictions and maintaining thorough auditing records.

2.3.4 Privileged Access Management (PAM): Protecting Vital Accounts: PAM services are being used more frequently to regulate and keep an eye on privileged permissions on critical systems. This helps to make sure that high-level users, like supervisors, have access that is verifiable and capable of being controlled.

2.3.5 Zero Trust Security: Involves access being restricted according to least-privilege principles and regular authentication of identities.

2.3.6 AI and Analytics: AI is used to detect abnormal behavior and enhance security monitoring.

IAM in IoHT networks is centered on integrating improved authentication, guaranteeing regulatory compliance, and protecting an increasing spectrum of devices that are interconnected. But issues like compatibility with old systems, scalability, and diversity of devices continue to be major worries. IAM approaches will need to be modified as IoHT networks diversify in order to maintain strong security and facilitate effective healthcare processing.

2.4 Issues present in IAM in IoHT networks

The special and complicated characteristics of healthcare environments—which include a variety of old technologies, strict laws and regulations, and a wide range of linked devices—give shape to the IAM problems that exist in IoHT networks. The following are the primary challenges associated with IAM for IoHT networks:

2.4.1 Device Diversity: Implementing consistent identity and access management throughout every hardware component is challenging since IoHT networks are made up of a diverse range of devices, each with unique security standards and characteristics.

2.4.2 Scalability: IAM systems experience difficulties expanding to effectively handle and verify a high volume of identities, both device-based and human-based, as the total number of internet-connected gadgets escalates.

2.4.3 Integration of Legacy Systems: A lot of healthcare companies continue to operate with older technologies that are hard to connect with newer Identity and Access Management (IAM) approaches, leaving safety and administration vulnerabilities.

2.4.4 Lack of Standardization: The authentication and maintenance of identifiers across various platforms and devices is inaccurate due to the absence of a common framework for IoHT device identity management.

2.4.5 Violation of Privileged Access: One of the biggest obstacles to overcoming threats from inside the organization is regulating privileged accounts as well as making sure administrators or high-level users have appropriate access controls and monitoring.

2.4.6 Security and Privacy Risks: Because of the intricacy of IoHT networks, it can be difficult to ensure adherence to laws like HIPAA and GDPR, where unauthorized entry to confidential health information can have dire repercussions.

2.4.7 Device Lifecycle Complexity: In IoHT networks, devices regularly have to be upgraded or substituted which makes it more difficult to manage their identities as well as accessibility permissions in the course of time.

2.4.8 User experience vs security: Strong security measures must be balanced with the medical professionals' convenience in application, as excessively complicated login processes may disrupt vital healthcare activities.

These problems demonstrate how difficult it is to, secure IoHT networks using efficient IAM techniques.

2.5 Solving the current issues using ML and DL techniques

Organizations are evolving their approaches to address security, authorization of access, and managing identities with the use of AI and ML integrated into Identity and Access Management (IAM). IAM programs can develop into more smart, automated, and adaptable to changing threat landscapes, customer preferences, and legal necessities by utilizing AI and ML. Following are the ways by which AI and ML techniques can be leveraged for the solving the issues:

2.5.1 The automated Analysis of User Behavior

AI/ML Role: To generate comprehensive behavioral accounts, AI and ML models examine user behavior. With the use of these characteristics, IAM systems are able to identify anomalies in behavior, such as atypical access behavior or spurious attempts at authentication, which may indicate security vulnerabilities.

Example: When algorithms for discovering abnormalities identify unusual activity, such as a healthcare provider accessing patient data after hours, they immediately take preventative measures, such as limiting access or demanding further verification.

2.5.2 Authentication Based on Risk

AI/ML Role: To ascertain the necessary level of authentication, ML-powered IAM systems assess the current context (location, device kind, login patterns). We refer to this as risk-averse or adaptive authentication. Based on the degree of danger, the system modifies the security requirements to add an additional layer of security without sacrificing user comfort.

2.5.3 Privileged Access Management

Continuous monitoring of privileged accounts by AI techniques to spot potential vulnerabilities or intrusion by insiders.

2.5.4 Intelligent Access Provisioning

AI/ML Role: AI and ML automate provisioning and deprovisioning of user access based on role changes, job functions, or lifecycle events. AI tools can suggest appropriate access rights based on user roles and continuously update permissions as job roles evolve.

2.5.5 Behavioral Authentication and Password-free systems

AI/ML Role: By providing password less authentication techniques like biometrics, behavioral patterns, or token-based access, ML models are rendering conventional passwords outdated. User authentication is achieved by the smooth incorporation of behavioral biometrics, such as typing speed, speech detection, and keystroke behavior. Example: AI-driven identity and access management (IAM) could enable healthcare personnel to uniquely identify oneself without the need for login in healthcare institutions by observing how they utilize equipment or systems.

2.5.6 AI for Zero Trust Security (Continuous Access Monitoring)

AI/ML Role: Assuming that no user or device is automatically trusted, AI and ML constantly observe the actions of users throughout the entire network. Without depending on fixed regulations for access, AI techniques can ensure that accessibility is constantly provided or revoked based on risk by evaluating current time information along with user actions.

Example: Should a healthcare professional abruptly begin retrieving information from a different location or device, the AI system may detect this behavior right away and prevent connectivity until additional authentication is finished.

2.5.7 Adaptive Access Management

AI/ML Role: In dynamic contexts like the Internet of Things, conventional inactive procedures for managing access are unsuitable. Dynamic authorization, where access rights are continuously updated based on environmental factors including the user's function, equipment, and surroundings, is made possible by AI/ML-driven systems. Example: Depending on whether a doctor is working remotely or on-site, their access to patient records might be dynamically changed to improve cybersecurity without disrupting with the processes.

Identity management has evolved as a result of AI and ML's integration with IAM. It is now more intelligent, adaptable, and safe. Intelligent Access Management (IAM) solutions, with their AI-driven risk analysis, behavioral identification, discovering anomalies, and autonomous the provisioning process, can adapt quickly to the dynamic security requirements present in current settings such as the Internet of Things (IoHT), guaranteeing strong security while improving the interaction of users.

3

Challenges and Solutions

3.1 Challenges regarding availability of datasets

While there have been great breakthroughs with the integration of AI and ML into IAM, there have also been obstacles, mainly with regard to the availability of datasets for training and optimizing AI/ML models.

3.1.1 Limited Real-World Data: Because medical data is sensitive and private, there are few high-quality datasets available for training IAM systems, especially in IoHT situations

3.1.2 Privacy and Compliance Concerns: Obtaining vast, diversified datasets for AI model training without breaching rules regarding confidentiality is challenging because healthcare data is protected by legislation such as HIPAA.

3.1.3 Data Quality and Labeling: It can be challenging to train efficient machine learning models for behavioral assessment or identification of anomalies when there is insufficient or improper labeling in the data, even when it is available.

3.1.4 Unbalanced Datasets: Unbalanced datasets impact model accuracy because security-related incidents (such as insider threats and illegal access) are uncommon in comparison to regular operations

3.1.5 Generating Synthetic Data: When real data is scarce, synthetic data is occasionally employed to fill the gap. However, this method introduces distortions or imperfections which can affect the accuracy and dependability of AI/ML models.

The development of strong AI/ML-based Identity and Access Management (IAM) systems that can efficiently identify security threats and protect user privacy and data has been restricted by these issues.

3.2 Generative AI an upcoming technology in Smart Authentication

By generating synthetic data for model training and enhancing biometric systems, generative AI has excellent prospects for enhancing smart authentication. It is an innovative approach for improving the intelligence, security, and usability of authentication, particularly in settings with complex security requirements like finance and healthcare.

3.2.1 Behavioral Biometrics Authentication: It verifies user identities by utilizing behavioral characteristics such as cursor actions, touchscreen hand gestures and speed at which users' type.

Generative AI's role: By generating synthetic data on behaviors, Gen AI might develop algorithms to recognize legitimate users and discover anomalies. Additionally, over time, it can adjust to minute variations in user actions. Continuous authentication, for instance, based on the rhythm of your typing or how you swipe the screen.

3.2.2 Biometric Verification: (Face, Speech and Language and Fingerprint). It Authenticates users using their voice, fingerprints, or face features.

Generative AI's function: Gen AI improves biometric systems by producing artificial samples to train models, increasing precision, and identifying efforts at spoofing (such as deepfake assaults).

For example, GANs (Generative Adversarial Networks) can produce fictitious faces in order to teach facial recognition software to more accurately distinguish between attackers and legitimate users.

3.2.3 Authentication Based on Synthetic Data: Synthetic data is used in place of actual user data, which may be hard to come by because of privacy concerns, to enhance authentication systems.

Generative AI's function: In order to help AI models train more efficiently and increase security without gaining access to confidential personal information, Gen AI creates synthetic data that mimics actual consumer behavior and biometric data.

For example, artificial intelligence (AI) systems can produce fictitious login attempts in order to find weaknesses in procedures for authentication and increase attack resistance.

3.2.4 AI-Generated Factors for Multi-Factor Authentication (MFA): It examines identification using a variety of techniques for authentication, such as passwords, biometrics, and tokens.

Generative AI's role: By using actual time customer environment and actions to produce unique, adaptive identification elements, Gen AI can improve the adaptability and security of multi-factor authentication.

For example, AI might provide distinct behavioral tasks in real time that go beyond conventional MFA techniques, including needing specific hand motions or vocal instructions.

By generating more resilient, customized, and adaptive security mechanisms, generative AI is revolutionizing smart authentication. With smooth and evolving procedure for authentication, these artificial intelligence-based techniques enhance the user interaction while providing stronger defense against forthcoming dangers.

4

Conclusion and Future Road map

Advantages of using Generative AI for IAM via Smart Authentication:

1. Increased Efficiency: By training on a variety of dynamic datasets, generative AI models increase accuracy and boost the dependability of authentication systems.
2. Fraudulent activity Identification: IAM systems can proactively identify and react to fraudulent activities or fake actions by utilizing AI-generated simulations.
3. Adaptability: Generative AI-powered systems are able to modify authentication procedures in response to dynamic real-time circumstances such as gadgets, location as well as actions.
4. Continuous Learning: IAM systems can adapt and learn from new data continuously by employing generative models, which gradually enhance safety and security.

4.1 summary and key findings

Healthcare Security is becoming more critical with the rise of digital technologies and the Internet of Healthcare Things (IoHT), exposing healthcare systems to cyber threats like data breaches and ransomware. Traditional password-based authentication is insufficient to safeguard sensitive patient data and medical devices. Smart Authentication provides advanced security solutions, such as Multi-Factor Authentication (MFA), biometric authentication, risk-based, password less, and continuous authentication methods to ensure secure, adaptive access.

Sensitive patient data and medical equipment cannot be adequately protected using conventional password-based protection. Smart Authentication offers sophisticated privacy technologies to provide safe, flexible access, including biometric, risk-based, password-less, and multi-factor authentication (MFA).

By providing real-time behavioral analysis, individualized access management, and AI-powered threat evaluations, Generative Artificial Intelligence (Gen AI) has the potential to enhance smart authentication through enhancing customer service and cybersecurity. To effectively implement the potential of Gen AI in healthcare security, however, issues including data protection, integration with current systems, and ethical considerations must be resolved.

4.2 Future Road map of IAM

In order to improve security, expedite authentication, and automate identity access management, requires the gradual integration of AI and generative technologies. The main goals will be to advance context-aware and biometric authentication, protect confidentiality, achieve seamless integration, and employ ethical AI in all industries—particularly vital ones like healthcare.

4.3 Recommendations for implementation in IoHT network scenario

The goal of the future roadmap for IoHT security, smart authentication, and Gen AI integration is to build healthcare ecosystems that are more adaptable, safe, and robust. This entails developing global standards and ethical frameworks, increasing the usage of biometrics, improving IoHT device defenses, and utilizing AI and Gen AI for predictive security.

i. **AI-Powered Risk-Based Authentication:**

   Completely incorporate AI to provide context-aware, ongoing authentication that adapts to changing circumstances and maintains security with little need for human input.

ii. **Smart Multi-Factor Authentication (MFA):**

   Transform into AI-driven biometrics (speech, motions, and behavioral identification) password-less authentication methods that provide more secure, frictionless access.

iii. **Generative AI for Threat Detection and User Behavior Analysis:**

   Strengthen the identification of anomalies and user activity assessment by utilizing generative artificial intelligence (AI) to spot anomalous patterns and stop illegal login requests.

   Create AI systems with self-learning and evolving capabilities to identify new threats and take independent action, enabling predictive security for IAM systems.

   Generative AI technology is close to being fully implemented and used in real-world IAM applications. This technology is here to stay, even if it won't significantly alter the way that many IAM procedures operate.

   In light of this, generative AI will undoubtedly have a significant and positive influence on the user experience when engaging with IAM tools in a way that is effortless, effective, and seamless.

References

1. M. Adil et al., “Healthcare Internet of Things: Security Threats, Challenges, and Future Research Directions,” in IEEE Internet of Things Journal, vol. 11, no. 11, pp. 19046-19069, 1 June1, 2024, doi: 10.1109/JIOT.2024.3360289.

2. Moustafa Mamdouh, Ali Ismail Awad, Ashraf A.M. Khalaf, Hesham F.A. Hamed, “Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions,” Computers & Security, Volume 111, 2021, 102491, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102491. (https://www.sciencedirect.com/science/article/pii/S0167404821003151)

3. https://eviden.com/publications/digital-security-magazine/ai-and-cybersecurity/generative-ai-for- iam/

4. The Evolving Landscape of Identity and Access Management (IAM) https://medium.com/@foxpass28/the-evolving-landscape-of-identity-and-access-management- iam-abb49d7ae3c6

5. Optimizing Healthcare Delivery With Generative AI Advancements, https://www.veritis.com/case- studies/optimizing-healthcare-delivery-with-generative-ai-advancements/

6. Artificial Intelligence and Identity and Access Management , Leanne Debeurre,, March 8, 2024, Artificial Intelligence, https://www.radiantlogic.com/blog/artificial-intelligence-and-identity-and- access-management

7. Himanshu Verma, Naveen Chauhan, Lalit Kumar Awasthi, “A Comprehensive review of ‘Internet of Healthcare Things’: Networking aspects, technologies, services, applications, challenges, and security concerns,”, Computer Science Review, Volume 50, 2023, 100591, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2023.100591.,(https://www.sciencedirect.com/science/article/pii/ S1574013723000588)

8. Top 7 Identity and Access Management Challenges to Solve, Michael Chen | Content Strategist | April 9, 2024 https://www.oracle.com/security/identity-management/iam-challenges/

9. M. Adil et al., “Healthcare Internet of Things: Security Threats, Challenges, and Future Research Directions,” in IEEE Internet of Things Journal, vol. 11, no. 11, pp. 19046-19069, 1 June1, 2024, doi: 10.1109/JIOT.2024.3360289.

10. M. Weqar, S. Mehfuz, D. Gupta and S. Urooj, “Adaptive Switching Based Data-Communication Model for Internet of Healthcare Things Networks,” in IEEE Access, vol. 12, pp. 11530-11548, 2024, doi: 10.1109/ACCESS.2024.3354722

11. M. Weqar, S. Mehfuz and D. Gupta, “DNS Traffic Monitoring to Access Vulnerability in the Internet of Healthcare Things Networks: A Survey,” 2023 International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON), New Delhi, India, 2023, pp. 89-94, doi: 10.1109/REEDCON57544.2023.10150996.

12. C. Singh, R. . Thakkar, and J. . Warraich, “IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations”, EJENG, vol. 8, no. 4, pp. 30–38, Aug. 2023.

13. Kelly JT, Campbell KL, Gong E, Scuffham P. “The Internet of Things: Impact and Implications for Health Care Delivery”. J Med Internet Res. 2020 Nov 10;22(11):e20135. doi: 10.2196/20135. PMID: 33170132; PMCID: PMC7685921.

14. J. Chen, Y. Shi, C. Yi, H. Du, J. Kang and D. Niyato, “Generative AI-Driven Human Digital Twin in IoT-Healthcare: A Comprehensive Survey,” in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2024.3421918.

15. Edward Lu, Oracle Cloud World Las Vegas 2023: A deep dive into the future of Identity and Access Management,August31,2023,https://blogs.oracle.com/cloudsecurity/post/cloudworld-2023-future-of-iam

16. Generative AI (GenAI) Future Roadmap: □ã□Ri□ ,PSA- Jt. Director at National Informatics Center, August 20, 2024, https://www.linkedin.com/pulse/generative-ai-genai-future-roadmap-%C5%9D%C3%A3-i%C5%A7-kk%C5%AFl%C5%9Dh%C5%99%C4%99%C5%9D%C5%A7h%C3%A3--ycjxc/

17. https://www.eccouncil.org/cybersecurity-exchange/network-security/imagine-genz-iam-with-gen- ai/

National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

The National Centre of Excellence (NCoE) for Cybersecurity Technology Development is a joint initiative between the Ministry of Electronics & Information Technology (MeitY), Government of India, and the Data Security Council of India (DSCI). Its primary objective is to catalyze and accelerate cybersecurity technology development and entrepreneurship within the country. NCoE plays a crucial role in scaling up and advancing the cybersecurity ecosystem, focusing on various critical and emerging security areas. Equipped with stateof-the-art facilities, including advanced lab infrastructure and test beds, NCoE facilitates research, technology development, and solution validation for adoption across government and industrial sectors. Adopting a concerted strategy, NCoE endeavors to translate innovations and research into market-ready deployable solutions, thereby contributing to the evolution of an integrated technology stack comprising cutting-edge, homegrown security products and solutions.

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

DATA SECURITY COUNCIL OF INDIA

+91-120-4990253 | ncoe@dsci.in

https://www.n-coe.in/

4 Floor, NASSCOM Campus, Plot No. 7-10, Sector 126, Noida, UP -201303

Follow us on

@CoeNational
nationalcoe
nationalcoe
NationalCoE