The Interaction Between Artificial Intelligence and Identity & Access Management: An Empirical study

Ishaq Azhar Mohammed

Sr. Software Engineer & Department of Information Technology

Hyderabad, India

Abstract*-The main purpose of this paper is to explore the significance of identity and access management systems in different businesses. The IAM system typically consists of specified functions as an information security system. The essential role is authentication because it is capable of providing confirmation of user identification for service providers utilizing IAM [1]. The purpose of this article is to offer a review of intelligent authentication studies with regard to IAM systems. These studies are assessed in light of the proposed crucial components for intelligent authentication. According to the findings of this study, it's not possible to develop and deploy an authentication system that met all of the conditions [1]. To manage modern multifaceted IT environments, it is essential for users to have access to every application, system software, databases platform and so on with distinct identity and related responsibilities. This method requires users to remember many passwords and IT personnel to repeat work for each platform to provide and maintain users. This affects productivity and raises the danger of the user being able to access important data and other business resources inappropriately. An alternative is a comprehensive and smart solution to Identity and Access Management (IAM) integrated with artificial intelligence. Companies have been able to condense*
the many identities of each user into a couple or, preferably, one identity and establish a single set of responsibilities, rules, processes, and proof of that identity. This method substantially automates IAM utilizing artificial intelligence, which enhances user and IT efficiency and optimizes safety and compliance. This paper demonstrates how the intelligent IAM interacts with artificial intelligence to streamlines many important tasks such as identity management and user authentication.

Keywords: *Identity and Access Management (IAM), artificial intelligence, automation, Identity Management strategy, Access management, regulatory compliance, breach detection*

I. INTRODUCTION

Research shows that there isn't a single week that goes by without a new data breach making news. As per the Identity Theft Resource Center, data thefts in the USA reached an all-time record in the past 10 years, an increase exceeding 30% [2]. It is tempting to assume that this is the product of hackers from across the globe. But most instances are considerably closer to home and are frequently caused by a mixture of inadequate security features, software flaws, human mistakes, malevolent insiders and the misuse of access and privileges. Identity & Access Management is a key tool for many organizations in their fight towards cyber security. It is a good and comprehensive solution to prevent data violations and handle the risks associated with remote operation and Bringing Your Own Device. IAM is continuously developing across key tasks, such as data security, authentication, internal data synchronization, administration of customer contact preferences and fulfilling privacy standards [2,3]. No underestimation of the significance of a smart and mature IAM approach should be made. Many companies struggle with determining who will have accessibility to what information, leaving their systems exposed. According to a study conducted by Forrester, 83% of companies have no mature strategy to the IAM [3]. The likelihood of these companies experiencing data violation issues is double that of organizations with their IAM approach. The study also provides a clear link between better IAM methods and reduced safety risks, greater productivity, enhanced control of privileged activities and much lower financial losses. Its primary purpose is to explore the interaction between AI and IAM in improving cybersecurity and other operations features.

II. PROBLEM STATEMENT

The main problem solved by this paper is to build an understanding on how artificial intelligence works with Identity Access Management to address cybersecurity threats and other information security challenges. Cybercriminals learn how companies typically handle security and develop subtler techniques for network infiltration. Detecting illegal attempts of access needs careful examination, which is no longer possible for human surveillance. In response, companies are turning to artificial intelligence (AI) technology to adopt better IAM policies to enhance access security and to preserve user identity integrity [. It is time for the management of identity and access (IAM) to evolve. The idea of identity has been extended to encompass not just human users, but also gadgets and apps, thus creating a difficult position for those responsible for identity management. A typical business network has hundreds or even thousands of identities, each of which has its own range of issues that it must deal with on a daily basis [4,5]. The scenario gets more complicated when cloud services enable users to access networks from any place and devices and the images are entered by flexible or remote employees. When consumers, clients, or third parties gain access, enforcing IAM rules consistently becomes difficult, if not impossible, for IT teams to manage on their own.

III. LITERATURE REVIEW

A. IAM Protest on AI

When it comes to IAM, one problem is that users are sometimes granted network access depending on their position inside a business, yet employees seldom fit into a single role. They require specific one-time access, or any individual with a comparable job may wish to have slightly different kinds of access [6]. This leads to extremely complex tasks that often need coordination across many departments. Proper management therefore requires multiple employees across all organizational layers. This could result in a situation where person experiences questionable "security fatigue" as a consequence of the increased volume of technical data, a difficult decision-making process, and a lack of relevance to their normal job [6,7]. A badly maintained IAM infrastructure may spell disaster for companies.

B. How can AI fix this?

Although this is a frequent occurrence in many businesses, it is not deemed unnecessary. AI technologies have the potential to significantly aid in the implementation of successful IAM, alleviating a great deal of frustration. Such technologies will enable the maturity of undertakings from too technical access management to comprehensible access management at all levels of the company. Analytics coupled with artificial intelligence provide insights into attention and speech so that every technical and non-technical employee works longer and more economically. Modern technologies provide methods to get fresh insights and automate procedures that may dramatically speed up the current IAM conformity controls [8]. They will identify abnormalities and possible dangers, but not the need for a large staff of security advisors. This equips employees with the information needed to make proper decisions, both technical and non-technical [9]. Such development is important, especially for anti-money laundering and fraud detection, but also in countering business executive risks [9,10]. It opens the way from reactive access management to proactive or even corrective access administration. This results in businesses that are always up to date and always secure.

C. Artificial Intelligence Approach to IAM

Artificial Intelligence has developed effectively in the last few years because to its unique characteristics such as flexibility, scalability and the capacity to face new problems and minimize human efforts and involvement [10]. The technologies AI and Machine Learning may be an important help for successful IAM. These current solutions may help companies to evolve from too technical access control to access management that is comprehensible at all levels [11]. Modern technologies offer new insights and procedures that substantially speed up current IAM compliance checks. Without the need for a big group of safety specialists, they can identify abnormalities and possible risks. This provides the knowledge required for workers (technical and non-technical) to make the right choices. These developments are important, in particular in anti-money laundering and fraud detection, but also in the fight against the dangers of insiders [11]. This is why AI is a lever for improving the IAM workflow of companies and making the IAM process even more essential in cybersecurity and Identity and Access Management [11].

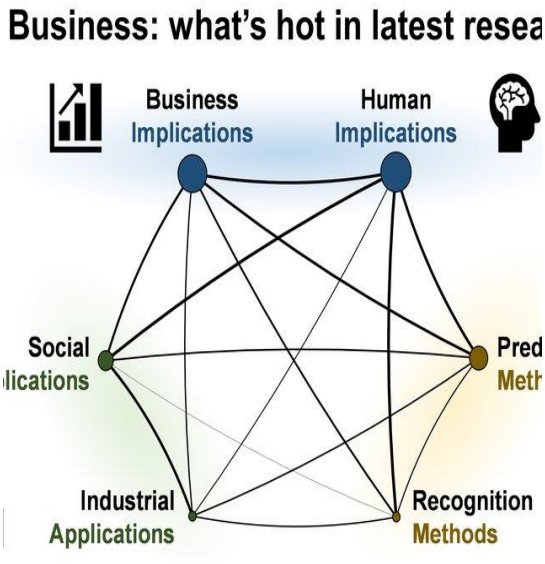

Fig i: IAM model for AI use in a business

D. How artificial intelligence transforms IAM?

1. AI monitoring and visibility improvement

By using AI, companies can keep an eye on everything at all times, and a computer can identify subtleties that humans cannot. Complex network interaction becomes apparent, enabling IT organizations to execute intelligent administrative actions and make better informed choices about user licenses [11, 12]. Role-based access may be upgraded to a more sophisticated approach with better management of privileged access and a less danger of privileged access misuse during periods in which temporary permissions are permitted [13]. The requirement for seamless, constant and accurate access to information is more essential as corporate systems are linked. Therefore, sophisticated authentication systems from AI will play an important role particularly if information is collected and analyzed much quicker than human beings. AI systems can continuously monitor users moving across the network within a user's access rights but can also detect any odd, illogical or changeable conduct. They might identify whether users would not typically visit a section of the system or retrieve more files than they usually do [13].

2. Automation and Flexibility

Because AI analyzes the intricacies of users' activities, authentication for low-risk access scenarios can be automated. Users will have less "security fatigue" as a result of this, as it relieves part of the stress of IAM administration [14]. AI is capable of examining the whole set of conditions around access requests, including the time of day, the kind of device being used, the position of the devices, and the assets being sought. While giving network access, it takes these considerations into account, which makes IAM relevant and granular, and it can manage possible issues caused by incorrect provisioning or deprovisioning of resources. In addition, Artificial intelligence systems are capable of applying suitable IAM guidelines to every access token depending on the requester's requirements and conditions, saving IT departments the time and effort of working out the fundamentals of "least privilege" for each use case on their own [14,15].

3. Increased effectiveness in ensuring regulatory compliance

Businesses that use enterprise software solutions that include artificial intelligence (AI) may improve the efficiency and efficacy of regulatory compliance procedures across a wide range of sectors. Many businesses think that adhering to security and privacy laws is adequate to maintain cybercriminals at bay, but this is not the case when it comes to meeting the requirements of their customers [16]. According

to the fundamentals of compliance, information should only be accessible by those who need it and should be rejected by everyone else. Establishing compliance requirements for new security legislation may be time-consuming, and noncompliance is a frequent occurrence in the industry. In these circumstances, the adaptive and flexible character of AI-powered IAM is advantageous. AI and machine learning are continuously monitoring traffic, learning user behaviors, and applying granular access restrictions [16]. As a result, businesses have less of a problem when enforcing security measures, and hackers have a more difficult time making use of compromised credentials.

Hackers are becoming more proficient and daring in their attempts to infiltrate networks these days. In order to detect illegal access attempts, thorough testing is required, which cannot be accomplished with precision by human monitoring [16]. This is one of the reasons why businesses depend on artificial intelligence technology to adopt better identity and access management procedures in order to improve access security while preserving the integrity of user identities. AI and machine learning combined with suitable monitoring and reporting technologies make it easier to monitor network connectivity and decrease total breach risk via the use of intelligent and adaptive IAM rules, which can then be implemented. In the highly competitive worlds of global finance and regulated sectors, investment in artificial intelligence may enhance the precision and reliability of compliance systems, as well as the overall effectiveness of the system [17].

E. Detection and prevention of data breaches

A further benefit of contextual monitoring is that it identifies abnormalities in user behavior that may suggest malicious intent or breach activities [17,18]. Machines are capable of handling huge quantities of data and scanning it at speeds that exceed the capabilities of even the most devoted IT staff. They can also warn businesses to odd activity in advance, allowing them to avoid severe network breach or data loss [18].By monitoring how various identities interact with corporate networks, data security integrating machine learning (ML) may "learn" aspects of user behavior [18,19]. As a result, the system can distinguish between what is normal and acceptable and what should be reported as suspicious behavior. Processes are carried out around the clock to provide continuous monitoring and to enable machine learning algorithms to build more accurate representations of regular network traffic. What occurs if a hacker manages to get access to the system using the identities of a legal user? During the session, the system detects any changes in behavior or odd actions and either notifies the IT department or reacts automatically by blocking access requests [18,19].

IV. FUTURE IN THE UNITED STATES

The interaction between AI and Identity management in the United States is more than just reacting to and exploiting current trends; it is also about facilitating the path that businesses are on as they transition to a digital world. A properly implemented Identity and Access Management system offers the basis for risk mitigation, better governance, and the development of a “Safe” Digital Enterprise [19]. In addition to automatic speech recognition as well as rules-based algorithms, artificial intelligence and cognitive computing are advancing to assist businesses in consuming and extracting value from large amounts of data, as well as driving governance and decision-making via the use of sophisticated analytics [19]. With regard to information and authentication management, this implies that far more sophisticated runtime authorization selections may be made utilizing the wealth of information that AI can ingest in order to improve decision granularity. Organizations like Elastic Beam, which was recently purchased by Ping Identity, have already started to use artificial intelligence (AI) for API behavioral security; Elastic Beam claims that AI-driven analysis is a more effective method of monitoring the increasing number of corporate APIs [19,20]. Although such algorithms seem to be accurate, there are concerns regarding their reliability, as well as whether or not they should be allowed to automatically ban people or APIs without human supervision.

V. ECONOMIC BENEFITS FOR THE UNITED STATES

The interplay between AI and IAM will have the most significant economic impact on the automation of activities that could not historically be automated. This will be economically beneficial to the U.S as it will certainly improve productivity and wealth creation. This will also have various effects on different kinds of employment, such as decreasing demand for some skills that can be automated while boosting need for other capabilities that are complimentary to artificial intelligence. According to the White House Council of Economic Advisors (CEA), automation will have the most detrimental impact on lower-paid employment, and there is a possibility that AI-driven automation would create more employment opportunities for the IT graduates. Public policy may mitigate the concerns of employment inequality by ensuring that people are retrained and capable of achieving excellence in professions that are complementary to, rather than competitive with, automated processes. 0] A public policy may also help to guarantee that the economic advantages generated by AI and IAM are distributed widely, and that AI is used responsibly to usher in an era of new prosperity in the global economy [2-. The fast development of artificial intelligence and information assurance has significantly raised the need for individuals with appropriate abilities to maintain and advance the fields. An increasing number of AI researchers are driving basic breakthroughs in artificial intelligence, a bigger number of experts are refining AI techniques for particular applications, and an even greater number of users are operating those applications in specific contexts. Artificial intelligence and information assurance training is intrinsically multidisciplinary, requiring a solid foundation in computer engineering, economics, programming environment, and evolutionary computation for researchers. A foundation in software engineering as well as knowledge of the application field is usually required for specialized training. Users must be acquainted with artificial intelligence and identity and access management systems in order to use AI technologies reliably.

VI. CONCLUSION

The purpose of this article was to examine the relationship between artificial intelligence and identity and access management. The findings from this research show that artificial intelligence is no longer a nebulous, future concept that no one can practically apply; but, the majority of companies have not yet matured in their approach to information and asset management. Businesses must begin to integrate smarter technology into their security procedures as a result of increased interconnectedness, an increase in the number of human and device identities, and the move toward worldwide access. When artificial intelligence and IAM are combined with suitable monitoring and reporting technologies, it becomes possible to visualize connectivity and ultimately reduce breaches exposure by implementing intelligent, adaptive identity and access management rules. For financial institutions, the question of identification has played a major part in the conduct of their operations. For banks to remain competitive in this changing environment, it is essential that they develop robust and reliable digital identification schemes that complement their existing

experience in confirming identities in the real world. On the road to converting the analog world's implemented sustainable to the virtual environment, there are many roadblocks to overcome, such as a lack of security, lack of interoperability, cyber assaults, and a lack of user access control. Businesses and governments must be able to develop solutions that safeguard consumers and maintain the privacy and security of their personal information while still offering more convenient goods and services.

.

REFERENCES

[1] C. Gunter, D. Liebovitz and B. Malin, "Experience-Based Access Management: A Life-Cycle Framework for Identity and Access Management Systems", IEEE Security & Privacy Magazine, vol. 9, no. 5, pp. 48-55, 2011.

[2] M. Bezzi, M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen and K. Zhang, Privacy and Identity Management for Life. Berlin: Springer, 2010.

[3] K. Bryson, M. Luck, M. Joy and D. Jones, "Agent interaction for bioinformatics data management", Applied Artificial Intelligence, vol. 15, no. 10, pp. 917-947, 2001. Available: 10.1080/088395101753242688.

[4] D. Cole, "Artificial intelligence and personal identity", Synthese, vol. 88, no. 3, pp. 399-417, 1991. Available: 10.1007/bf00413555.

[5] N. Sgouros, "Interaction between physical and design knowledge in design from physical principles", Engineering Applications of Artificial Intelligence, vol. 11, no. 4, pp. 449-459, 1998. Available: 10.1016/s0952-1976(98)00037-2.

[6] Arabo, User-centred and context-aware identity management in mobile ad-hoc networks. Cambridge Scholars Publishing, 2013.

[7] R. Sharman, S. Smith and M. Gupta, Digital identity and access management. Hershey, Pa.: IGI Global (701 E. Chocolate Avenue, Hershey, Pennsylvania, 17033, USA), 2012.

[8] N. Berlatsky, Artificial intelligence. Detroit: Greenhaven Press, 2011.

[9] M. Bramer, Research and Development in Intelligent Systems XXVII. London: Springer-Verlag London Limited, 2011.

[10] M. Stefik, "Artificial intelligence applications for business management", Artificial Intelligence, vol. 28, no. 3, pp. 345-348, 1986. Available: 10.1016/0004-3702(86)90055-x.

[11] C. Tappert and N. Dixon, "A procedure for adaptive control of the interaction between acoustic classification and linguistic decoding in automatic recognition of continuous speech", Artificial Intelligence, vol. 5, no. 2, pp. 95-113, 1974. Available: 10.1016/0004-3702(74)90025-3.

[12] S. Fischer-Hübner, S. Furnell and C. Lambrinoudakis, Trust, privacy, and security in digital business. Berlin: Springer, 2006.

[13] W. Bainbridge, *Online worlds: convergence of the real and the virtual*. London: Springer, 2010.

[14] K. Frankish and W. Ramsey, The Cambridge handbook of artificial intelligence. London: Cambridge University Press, 2014.

[15] B. L?opez, M. Polit and T. Talbert, Artificial Intelligence Research and Development. Amsterdam: IOS Press, 2006.

[16] R. Lee, Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. Cambridge University Press, 2014.

[17] T. Winograd, "Shifting viewpoints: Artificial intelligence and human–computer interaction", Artificial Intelligence, vol. 170, no. 18, pp. 1256-1258, 2006. Available: 10.1016/j.artint.2006.10.011.

[18] M. Weske, C. Godart and M. Hacid, Web Information Systems Engineering WISE 2007 Workshops. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2007.

[19] J. Balmer and S. Greyser, "Managing the Multiple Identities of the Corporation", California Management Review, vol. 44, no. 3, pp. 72-86, 2002.

[20] B. L?opez, M. Polit and T. Talbert, Artificial Intelligence Research and Development. Amsterdam: IOS Press, 2006.