IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Identity Management Capability Powered by Artificial Intelligence to Transform the Way User Access Privileges Are Managed, Monitored and Controlled

Ishaq Azhar Mohammed

Sr. Data Scientist & Department of Information Technology

Dubai, UAE

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

Keywords: Management of identity and access, artificial intelligence, biometrics and IAM systems, managing identity.

I. INTRODUCTION

The intelligent solution of the next generation IT operations increases the accuracy and speed of near-real-time access rights for digital identification. The patent-pending IAM feature reduces the complexity of controlling and monitoring who has access to what by aggregating data from various systems and sources. It enhances and boosts the exactness and speed of almost real-time user privileges updates via artificial intelligence and machine learning to contextualize identification choices and keep up with constantly changing changes in user rights of access [2]. This helps businesses to identify regions of greater risk proactively, which may need further management, eliminating the requirement for error-prone manual provisioning of today's IAM solutions. In managing user rights, access provision should be based on accurate information about who a person is and why they need it. The problem is that current access control methods are based on assumptions rather than a full amount of knowledge. With our IAM capabilities, we have developed a proactive Identity Management strategy that helps to minimize human error and costs and enhances risk awareness, and eases identification of outliers. Integrated solutions utilizing state-of-the-art analytics and artificial intelligence (AI) offer improved functions and safety to swinging doors and towers [2]. The rapid growth of video-associated technologies with improved capacity, owing to better analytics, has frequently dominated over the last decade. Due to the ongoing pandemic issue, however, the traditional access control industry has become well-known in the last year. Integrated systems are building on advances in artificial intelligence (AI) solutions that speed up the creation of cloud integration platforms and an increasing inventory of mobile devices, touchless and biometric features. While AI is becoming an essential element of corporate activities in a variety of market sectors across the world, security applications have been developed to consider it. Nevertheless, the additional health concerns facing businesses today have pushed security solutions vendors and consumers to reconsider how AI might assist reduce these threats [3]. There is little dispute that AI might significantly improve the safety of external and internal entries, as used in the short term during this crisis. But, while AI can help with a range of security activities, like distinguishing individuals and objects within the perimeter and interior of a facility, identifying planned piggybacking, detecting and evaluating potentially deadly objects and harmful people and much more, AI algorithms alone may not start acting to avoid unauthorized of people or to avoid harmful objects from entering. This presentation will thus allow us to better understand how AI works to increase IAM capability via an IBM AI identity management technology possible scenario [4]. This paper will explore extensively the applications of AI in identity and access management especially monitoring, managing, and control of access privileges.

II. PROBLEM STATEMENT

The main problem that this research will address is how artificial intelligence is crucial in enhancing identity management capabilities to change the privileges of access managed, monitored, and controlled by way of users. As access rights spanning tens of thousands of workers and apps are increasing, many big companies struggle to manage and protect the smooth nature of user privileges [4]. The patent-pendent IAM feature reduces the complexity of controlling and monitoring who has access to what by aggregating data from various systems and sources. It enhances and boosts the precision and speed of near-real-time updates to user rights via artificial intelligence and machine learning to contextualize identification choices and keep up with constant changes to user rights of access. This will enable businesses to proactively identify areas of greater risk that may need additional governance to decrease the need to provide today's IAM systems with error-prone manual procedures [4,5]. Low confidence rates suggest potentially dangerous access, and for automated approvals, high confidence ratings may be considered to relieve individuals with human approvals from focusing on unique models and risky outliers. It may also anticipate and suggest the need for new joiners in a business to save time, money, and effort in the integration process.

III. LITERATURE REVIEW

A. Identity Management AI

Businesses are struggling to cope with the constantly increasing number of malicious access from unauthorized people from within and outside attempting to get access to corporate networks, and they are looking for innovative methods to counter these digital threats [5]. The solution is artificial intelligence. The automation of the identity access process by employing artificial intelligence (especially machine learning, and deep learning) provides IT experts with the capacity to detect data breaches in real-time, allowing them to ensure that users are exposed to just the content and services that they require [5]. By incorporating artificial intelligence, the strategy becomes faster and more effective, as the software "learns" human behavior patterns, resulting in time savings and improved outcomes. The IAM capacity produces a confidence score for each user to assist decide efficient and secure access to the data, and constantly monitor access to ensure that the score is updated often [6]. Low confidence ratings suggest potentially dangerous access and automated approvals may be assessed as high confidence ratings that allow people carrying out human approvals to concentrate on odd designs and risky outliers. It may also forecast and suggest access requirements for new carpenters in a business to save time, money, and effort in the integration process [6].

While AI remains developing in IAM, IT teams and security experts need to assess how AI integration might improve their authentication environment. Many administrative duties may be performed by robots that interact with one another and adapt over time, increased automation such as biometrics. AI can provide proper security that goes beyond biometrics, allowing for a more comprehensive degree of access management [7,8]. This may involve the use of vision, audio, psychographic characteristics, and risk assessment.

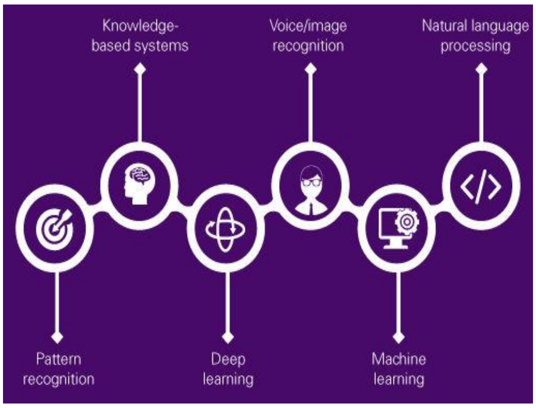

Fig i: AI capabilities

B. The Interaction Between Artificial Intelligence and Identity & Access Management

The identity and access management system (IAM) is a key weapon in the cybersecurity arsenal of many organizations. In addition to mitigating against data breaches, it also helps to manage the risks associated with remote working and bringing your device – BYOD – into the workplace. Internal data synchronization, customer contact preference management, and fulfilling privacy compliance standards are just a few of the important tasks that IAM is continuously developing to handle in the modern world [8]. It is important to recognize the significance of a well-thought-out and well-developed IAM strategy. Determining who should have access to what information is a tough decision for many companies, and this difficulty makes their information systems insecure. Forrester's study found that 83 percent of companies do not have a mature strategy to identity and access management (IAM). When compared to companies that have implemented their IAM strategy, these organizations are twice as likely to have difficulties as a result of a data breach [8]. A clear link is established between better IAM methods and decreased security risk, enhanced productivity, greater privileged activity control, and significantly reduced financial loss [10].

C. Using Artificial Intelligence in IAM: An Approach

Machine Learning has progressed effectively over the last few years as a result of its unique characteristics such as flexibility, scalability, and the capacity to deal with unforeseen problems while reducing the need for human involvement and effort. Artificial Intelligence and Machine Learning technologies have the potential to be a major support for successful IAM [11]. These cutting-edge solutions may help businesses transition away from too technical access control and toward access management that is comprehensible on all levels.

Modern technologies allow for the discovery of new insights and the automation of processes, which substantially speeds up the existing IAM compliance controls and reduces their overall time to market. There is no need for a big staff of security specialists to identify abnormalities and possible dangers since they can do so on their own [12]. Thus, both technical and non-technical workers have the knowledge they need to make informed choices. Such advancements are critical, particularly in the areas of anti-money laundering and fraud detection, but also in the areas of insider threat mitigation and prevention. Therefore, it is possible to argue that artificial intelligence can be used as a lever to enhance the IAM process in businesses and that this capacity makes it more essential in cybersecurity and Identity and Access Management [13].The benefits of AI in IAM are as follows:

1. ***Increased visibility as a result of artificial intelligence monitoring***

It will become more essential as corporate systems grow more linked to ensure that information is accessible in a smooth, continuous, and accurate manner. As a result, artificial intelligence-based enhanced authentication systems will play a significant role, particularly when it comes to gathering and processing information much more quickly than humans [13]. As long as AI systems are operating within the parameters of a user's access rights, they could continuously track users' movements throughout the network, but they could also monitor any odd, illogical, or changeable behavior shown by users. They might tell whether people are attempting to access a section of the system that they would not usually access or if they are downloading more documents than they would regularly download.

2. ***Automated and adaptable processes***

Because artificial intelligence keeps track of the specifics of users' activities, it is feasible to automate authentication for low-risk access scenarios in certain cases. In this manner, it may relieve some of the efforts of IAM management while also preventing users from experiencing "security weariness." 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 location of the device, and the resources being sought [13]. Before giving network access, it takes these considerations into account, which makes IAM contextual and granular, and it can manage possible issues caused by incorrect provisioning or de-provisioning of resources. In addition, AI-powered systems are capable of applying suitable IAM rules to every access request 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 [13,14].

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 sufficient to keep hackers at bay, but this is not the case when it comes to meeting the requirements of their customers [14]. According to the fundamentals of compliance, information should only be accessible by those who need it and should be rejected by everyone else. Implementing 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. 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 [14].

Hackers are becoming more proficient and daring in their attempts to infiltrate networks these days. To detect illegal access attempts, a thorough examination is required, which cannot be accomplished with precision by human monitoring. This is one of the reasons why businesses depend on artificial intelligence technology to adopt better identity and access management procedures to improve access security while preserving the integrity of user identities [14]. AI and machine learning combined with suitable monitoring and reporting technologies make it possible to visualize network access and decrease total breach risk via the use of intelligent and adaptive IAM rules, which can then be implemented. When it comes to the highly competitive world of global banking and regulated sectors, investing in artificial intelligence and machine learning may improve the accuracy and efficiency of compliance systems, among other things [14].

D. IBM AI Identity Management Innovations

IBM (NYSE: IBM) Artificial Intelligence security (AI) technology was initially designed to safeguard financial service customers, via an IDaaS (identity-as-a-service offering) to clients in various sectors [15]. IBM Cloud Identity now has adaptive IA-based access capabilities that continuously evaluate the risk levels of employees or consumers while they are reaching apps and services. The system increases suspicious user interactions for additional authentication, while those classified as low risks are "tracked quickly" so that they may access their required apps and services [15]. Traditional methods of secure access, such as passwords, are frequently not adequate to prevent unwanted access with increasing data breaches. The increase in the number of credentials, when a malicious actor receives a list of credentials and tests them on different other sites using a bot, shows that many password combinations have been exposed. According to a 2018 study, the reason of more than 80 percent of data breaches are hacked and weak credentials. Meanwhile, data from 2017 showed that big businesses manage hundreds of apps - up to 788 individual applications for companies with over 50,000 workers on average [15]. Given the number of applications and passwords that workers manage between their working and personal life, new security measures are increasingly essential to avoid hindering user experience." Companies continually strive to improve security and user experience, but the key is to ensure that security does not interfere with daily user journeys. Cloud Adaptive Identity uses AI to provide organizations with a holistic view of user access contexts based on indicators such as malware and risk indicators, device insights, and user behavior, to help them focus safety on high-risk logins and allow most users seamless access to account and applications [15].

E. Adaptive Access: Intelligent Context

Many businesses continue to depend on outdated username and password systems for providing access to services for employees and consumers. Because of the hodgepodge of apps and solutions, companies may not be able to implement more contemporary security layers [16]. This may create a blind point that hinders security teams from simply establishing rules that flag suspected indications, such as unfamiliar locations, unknown devices, and if a user is on a company's VPN network.

IBM Cloud Identification is a service identity solution that supports businesses with adaptive access connecting all users to all applications. By using AI, the solution facilitates access control and user security by assigning user risk levels based on specified criteria. With these risk levels, administrators may design rules that authenticate up or down, and use strong authentication only when necessary [16]. The service uses the following characteristics to identify risks and to allow adaptive access decisions:

- **Artificial Intelligence:** a user behavior score should be given based on the degree of confidence or risk evaluated for each user. A variety of variables, including online intelligence, location information, malware, and danger indicators and device insights, have been evaluated. For example, AI may be used to identify abnormal mouse movies or to alert a person who attempts to log in from a malware-infected browser. IBM Cloud Adaptive Access Identity uses IBM Trusteer AI technology to evaluate users using a fraudulent evidence base, fraudulent pattern analysis, and organizational patterning [16].

- **Smart Access and Seamless Login:** As AI capabilities may allocate risk levels, only more threatened users are prompted by authentication via multifactor or refused access. By asking selected individuals to verify their identity further rather than all users, businesses may minimize operating costs for things such as double-factor authentication and assist password resets for both new and existing users. This may contribute to cost reductions since companies across various industries have budgeted more than $1 million per year for password-related assistance alone [16].

- **Low-code Deployment:** Applications and APIs may have adaptive access rules developed and deployed with little or no development work, and without modifications in apps [16].

IV. FUTURE OF RESEARCH

Identity and Access Management (IAM) by AI is destined, as technology and the social environment continue to shift quickly, to be a more and more essential part of our personal and corporate life. Identity management and Artificial Intelligence will change security beyond people, places, and things we control now because a growing number of devices and systems interact with one another without human involvement and learn from one another [17]. While we cannot foresee anything incomplete and precisely beyond the near future, technology is expected to continue changing our lives in years to come, demanding a new identity and access management strategy. IBM Security provides one of the most sophisticated and comprehensive company's security solutions and services portfolios. Supported by world-renowned IBM X-Force® research, this portfolio allows companies to manage risk efficiently and to protect themselves from new threats [18]. With numbers increasingly dispersed and linked systems, smooth, continuous, and correct access to all resources is common via sophisticated authentication methods, such as biometrics and artificial intelligence technologies. Password is the stuff of the past because machine-controlled access management will replace human-controlled access. There will no longer be passwords to enter buildings for accessing systems or badges [18]. When using ATMs, entering shops and restaurants, visiting online websites, entering office spaces, driving vehicles, and using business systems, intelligent systems will be able to identify and welcome us by some of our personal and unique characteristics.

V. ECONOMIC BENEFITS

From an economic perspective, the idea of distributed and verified identification will be embraced by every commodity, business, and system in the United States in the near future. A person may have many identities but is still recognized as the person and the identities of intelligent things are connected to people who possess them. Global identification service providers register identities and manage identity directories with the growing number of extremely powerful identities [18]. Biometric technology is progressing fast, and according to different research studies, the market for biometric systems is expected to grow from 10 billion USD in 2015 to about 40 trillion USD by 2022. Artificial intelligence integrated into the future IAM products will be able to find out the user and user actions will be evaluated and abnormalities will be automatically notified. The fast-technological developments and massive data dumping by robots will need future identities and access management experts to have analytical and critical thinking abilities to select relevant data and to understand all the reporting data of the machine [18]. This will boost job possibilities and sales from robotic manufacturing.

VI. CONCLUSION

This paper focused on understanding how AI works to improve IAM capabilities with a case scenario of IBM AI innovations for identity management. Identity Management of identity and access and artificial intelligence are all essential elements of today's digital transformation initiatives. The study results show that, since applications and data files that include sensitive and personal information are increasingly being stored in the cloud, it is essential that all steps be taken to protect cloud assets to avoid system infringement and data loss. AI-powered identity and access management (IAM) are one of the most effective methods of providing security. Artificial intelligence is a double-edged sword that may be exploited by hackers as a safety solution or as a gun. AI involves the development of algorithms and systems capable of showing human behavioral features. Features include the capacity to adapt to a certain environment or to react to a situation intelligently. Cybersecurity solutions have been used widely by AI technologies, but hackers also use them to build smart malware programs and perform rocket attacks.

REFERENCES

[1] L. Benyoucef and V. Jain, "Editorial note for the special issue on 'Artificial Intelligence Techniques for Supply Chain Management'", Engineering Applications of Artificial Intelligence, vol. 22, no. 6, pp. 829-831, 2009.

[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] 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.

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

[5] 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.

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

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

[8] 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.

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

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

[11] 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.

[12] 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.

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

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

[15] C. Chan and G. Huang, "Artificial intelligence for management and control of pollution minimization and mitigation processes", Engineering Applications of Artificial Intelligence, vol. 16, no. 2, pp. 75-90, 2003.

[16] S. Dunn, "Identity Manipulation: Responding to Advances in Artificial Intelligence and Robotics", SSRN Electronic Journal, 2020.

[17] M. Lauras and T. Comes, "Special Issue on Innovative Artificial Intelligence Solutions for Crisis Management", Engineering Applications of Artificial Intelligence, vol. 46, pp. 287-288, 2015.

[18] M. Stefik, "Artificial intelligence applications for business management", Artificial Intelligence, vol. 28, no. 3, pp. 345-348, 1986.

[19] S. Zeadally, E. Adi, Z. Baig and I. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity", IEEE Access, vol. 8, pp. 23817-23837, 2020.