A literature review on the application of AI to Identity Access Management

Ishaq Azhar Mohammed

Sr. Data Scientist & Department of Information Technology

Dubai, UAE

Abstract*-The main focus of this research is to explore how artificial intelligence may be used in the context of identity and access management. The identity and access management system (IAM) is a prime requisite in the cybersecurity arsenal of many organizations. In addition to mitigating against data breaches, it also helps to manage the risks associated with working remotely 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 [1]. It is important to recognize the significance of a well-thought-out and well-developed IAM strategy. Determining who should have accessibility 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 companies are twice as likely to have difficulties as a result of a security breach [1]. A clear positive correlation has been found between better IAM methods and decreased security risk, enhanced productivity, greater privileged activity control, and significantly reduced financial loss, according to the study.*

Keywords: *Identity and Access Management (IAM), artificial intelligence, automation, Internet of Things (IoT), Multi-Factor Authentication (MFA)*

I. INTRODUCTION

Among the most critical challenges of information, security is creating a trusted authentication mechanism based on the digitalization of identity. Identities are described as a set of well-
defined characteristics that distinguish one thing from another when compared to other entities [1]. While a digital identity is a collection of characteristics held by an entity and utilized by information systems to represent identity, a digital signature is a collection of characteristics owned by an individual [1]. Its administration is usually outsourced to Identity and Access Management (IAM), which ensures that the appropriate people have access to the appropriate assets at the appropriate times and for the appropriate reasons [2]. A total of three sub-tasks are involved in user authentication (identification, enrolment, and verification). Specifically, the first and second sub-tasks are concerned with the creation and registering of digital characteristics associated with users that will be utilized in the verification process. Such specifications and configurations are often set as part of the arrangement between IAM and network operators, which may be found here. Whenever a user tries to access a service provider system through IAM, the last job that is performed is called the final task. As a result, the verification process is an important stage in any kind of authentication system since it establishes the identity of the user and determines whether or not he has been successfully authorized. Conventional authentication is dependent on a variety of variables, and both knowing-based and possession-based techniques suffer from a variety of problems. Using the example of a password authentication technique, the revealed users' secret phrase (password), as well as the secret phrase that has been stored in the system, are simply compared [1]. The outcome of this matching process is utilized to establish the identification of the claimed user in question. There are many issues with this method, including the possibility of the secret phrase being stolen or forged. This paper will examine how artificial intelligence is being used in identity and access management, as well as the challenges that have been encountered and the industry's future.

II. PROBLEM STATEMENT

The main problem that this research will seek to resolve is to explore how artificial intelligence (AI) plays a vital role in information assurance and management (IAM). Signs of malicious behaviour include malicious logins, high numbers of login attempt in a short period, unfamiliar sites, unauthorized technologies, and whether or not a user is connected to the firm's virtual private network (VPN) 3, [4]. To prevent attempted attacks, artificial intelligence may flag these indications for examination in real or near-real-time. Identity and access management (IAM) is becoming more reliant on artificial intelligence (AI), which allows businesses to adopt a far more detailed and adaptable response to authentication and access control as a result [4]. In addition, artificial intelligence (AI) is required for user and entity behavior analytics (UEBA), which is used to detect suspicious activities. Authentication and access control are required for data security. When correctly deployed, IAM systems may improve employees' performance by enabling access to data via different applications, places, and devices [4]. It also makes it possible to collaborate more effectively with other companies, suppliers, and commercial partners. Auditing current and outdated networks before installing an IAM solution is the most effective method. Identifying gaps and opportunities, as well as collaborating with stakeholders early and often, are essential [4]. Create a comprehensive list of all user categories and access situations, as well as a core set of requirements that the IAM solution must satisfy.

III. LITERATURE REVIEW

A. Identity and access management (IAM)

Identity and Access Management (IAM) is a broad term that refers to the framework of rules and technology used to guarantee that authorized individuals within an entity have proper network access [5]. Access control to a company's assets is provided through identity management systems, which also monitor user behavior while they are logged into those resources. The IAM enables the management of user authorizations depending on their organizational roles [5]. This is accomplished by providing a method of safeguarding

organizational resources and data via rules and regulations that require login passwords, define user rights, and control user accounts, among other features. IAM is a process of integrating workflow systems that includes organizational think tanks that evaluate and improve the effectiveness of security systems [6]. Standards, processes, regulations, and procedures are all intertwined with information assurance management. Applications for identity and security management are also essential concerns. Access requests to secured business documents are verified by IAM, and users are either granted or denied access based on their results. It also handles a variety of administrative tasks, such as password issues, and assists with the oversight of employee identity management systems. The management of user life cycles, different application accesses, and single logons are all examples of IAM standards and applications [6,7]. There are many benefits to using IAM, including improved business value and security, better work efficiency, and a decrease in the burden of IT personnel. The organization uses IAM to ensure that they comply with professional standards, whether they are in the health, banking, or other industries [8]. As more companies embrace interoperability insensitive records systems, record security becomes more essential [9].

Employees are no longer the only ones who benefit from IAM. Contracting companies and business partners, distant and mobile users, as well as consumers, must be able to access company resources securely. With digitization, identities are allocated to the Internet of Things (IoT) devices, robots, and bits of code, such as APIs or microservices, as well as to people and organizations [10]. Multicloud hybrid IT systems and software as a service (SaaS) solutions add to the complexity of the identity and access management (IAM) landscape. When implemented properly, information asset management (IAM) helps to guarantee corporate efficiency and the smooth operation of digital systems. Employees may work smoothly from any location, while centralized administration ensures that they only have access to the resources that are necessary for their tasks. Additionally, making systems more accessible to consumers, contractors, and suppliers may improve productivity while decreasing costs [10].

B. Making Use of Artificial Intelligence

As many people prepare to find employment, one thing is certain: it has compelled executives across all sectors to reconsider the nature of the working environment and technology–both physically and in terms of security–because of the events of September 11. For others, this means the end of lecture halls, desk partitions, temperature checks, and rotational days, during which office employees must adhere to strict rules about when they walk in and how they utilize various areas [11].

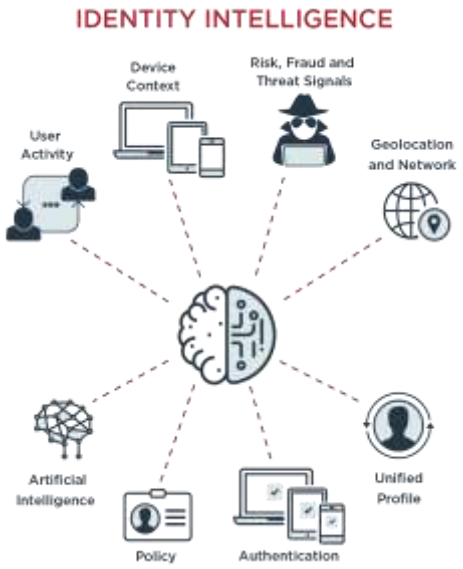

Fig i: IAM platform utilizing AI

C. Remote work is here to stay

Bearing in mind that remote work and technology are feasible and don't impact productivity, some employees may never really return to physical workplaces. According to a recent study of finance executives conducted by the research company Gartner, 74 percent of respondents want to permanently transfer certain workers to remote work [11] The IT and security personnel will need to accurately describe their information protection rules related to remote work that were either put in place or at the very least reviewed at the outset of the migration to a virtual workforce for those employees who will continue working from home [11]. In any case, businesses must consider how to increase employee flexibility while still providing them with the necessary technology and resources to continue working effectively and safely during times of transition.

D. Identity is at the heart of everything.

Identification and Access Management (IAM) systems, such as OneLogin, put identity at the heart of how people engage with digital content [12]. Modern identity and access management (IAM) systems are continuing to investigate the potential of artificial intelligence (AI) to offer login experiences that are more frictionless while still being safe. The use of artificial intelligence (AI) by cybercriminals to conduct increasingly automated and broad assaults that target especially susceptible sectors or systems, such as overburdened hospitals or online learning programs, is also becoming more common. The obvious reaction would be to restrict access control to the maximum extent feasible, forcing users to authenticate several times throughout the day using Multi-Factor Authentication (MFA) whenever they require access to their apps [12]. While an IAM system may enable you to implement such security rules, not all can dynamically raise or reduce authentication requirements as needed.

E. Artificial intelligence for risk-based authentication

It is at this point that risk-based authentication comes into play. To establish a user or transaction's risk profile and suitable process, risk-based authentication uses contextual variables like time, place, search engine, and device [13]. OneLogin Authentication from OneLogin accomplishes this:

• For high-risk logins, administrators may demand users to provide an extra authentication factor, such as a Face ID or fingerprint scanning, or they can completely refuse them access to their online platform.

• For low-risk logins, when users behave predictably, administrators may just demand the submission of an OTP number received via phone or enable the user to skip MFA altogether if they want.

In essence, it's a win-win situation. When the context of a user's login changes substantially, MFA or other authentication factors must be used to prevent phishing and ransomware attacks.

F. Challenges and risks of implementing IAM

Even though IAM is present at every level of an organization's information security architecture, it does not cover all of the bases. One problem is the evolution of users' "birthright access" rules [13,14]. These are the access privileges granted to new users during their first day of employment at a business. When it comes to granting access to new workers, contractors, and partners, the choices are many and touch on a variety of different departments. This degree of automation becomes critical when considering automated onboarding and compliance management of users, user self-service, and ongoing verification of compliance, according to Steve Brasen, research director at the European Medicines Agency, who wrote about it in a blog post. It is not possible to manually change access rights and restrictions for hundreds or thousands of users at the same time [14]. Having no automatic "leave" procedures (and without reviewing them regularly) will virtually ensure that unnecessary access privileges will not be fully removed. Another problem is that, although zero-trust networks are quite popular right now, the challenge is being able to constantly monitor these trust connections when new applications are introduced to a corporation's IT system architecture. We must monitor what individuals do after logging in and examine the baselines of behavior. There are many false positive scenarios, such as if a user breaks their finger that may destabilize these trust connections. Following that, the connection between identity and access management (IAM) and single sign-on (SSO) must be properly managed [15,16]. The integration of identity and access management with customer-centric identity and access management has started, as shown by Okta's purchase of Auth0 [16]. Because security experts will continue to treat these initiatives separately, IAM will be forced to play catch-up all of the time.

Following that, IAM personnel should be familiar with a variety of cloud architectures. One may see cases of IAM security best business practices for Amazon Web Services (AWS), Google Cloud Platform, and Microsoft Azure in the following sections [16]. It will be difficult to integrate these practices with an organization's network and applications infrastructure, and it will be much more difficult to close the security gaps that exist across various cloud providers.

Finally, IT administrators must include identity management in the development of all new apps from the beginning. To successfully pilot any IAM and identity governance initiatives by carefully choosing a target app that can be used as a template and subsequently expanded to additional applications throughout the business.

How Artificial Intelligence Addresses IAM Challenges

Even though this is a fairly frequent occurrence in many businesses, it is not necessary to remain in this state. Artificial intelligence (AI) may be a major aid in achieving successful IAM, and a great deal of aggravation could be alleviated. As a result of these technologies, businesses will be able to transition from too technical access management to access management that is comprehensible at all levels of the organization [17]. Analytics coupled with artificial intelligence will provide focus and discourse insights, allowing both technical and non-technical employees to work for extended periods while being productive. New insights may be gained via the use of cutting-edge technology, and procedures can be automated, allowing for a significant speedup in the current IAM compliance controls. They will identify abnormalities and possible dangers without the need for a large staff of security experts to do the same task.

This equips employees, both technical and non-technical, with the information they need to make the best decisions possible. The need for such development is critical, especially in the areas of anti-money laundering and known security vulnerabilities, but also in the areas of countering business executive risks [17].

It opens the way for the transition from reactive access management to preventive or even corrective access management in the near future. Thus, businesses are always up to date and continually secure as a result of their efforts.

Elimity's approach to artificial intelligence in IAM

Elimity makes use of machine learning to provide insights into the present identity and access status of your company's IT infrastructure. Machine learning algorithms are very effective in detecting abnormalities and assisting with the establishment of a so-called baseline model, among other things. Within Elimity, this paradigm is converted into a set of rules. Then, in the context of particular audits or reporting activities, these rules may be validated by the relevant individuals. 7If necessary, the rules may be revised to better reflect the current circumstances inside the company and to take into consideration the firm's overall business strategy [1]. All of these guidelines, as well as any abnormalities that are found within the present condition, will be utilized in the assessment of all future reporting that occurs. We are not believers in the "big bang" approach to artificial intelligence. A great deal of business context and information is not covered by the tools and configuration, and as a result, it is difficult for it to be found automatically. We are firm believers in the additive function of artificial intelligence: we use machine learning as a virtual assistant alongside an expert, to aid in digging through data and discovering what is standard, as well as flagging anything out of the ordinary for human assessment. This virtual assistant will aid in automating the IAM controls to maintain more consistency in control.

IV. FUTURE IN THE U.S

In the United States, artificial intelligence and information and communications technology (ICT) are developing at breakneck speed. In the future of IAM, artificial intelligence (AI) will be critical since it can detect trends and grow knowledge exponentially – at the same pace as risk – allowing it to be more effective. This tendency must be carefully handled since millions of employees will be educated in the expectation that they will be retrained in the near future. It is not necessary to put a halt to technological progress, but it must be closely controlled and evaluated. Over the last several years, digital IDs have gained in popularity and have been used more widely, particularly inside national government organizations. The area of identity and access management has grown significantly in recent years, as remote work has become the standard and mobile device use has reached its maximum penetration. Because of the proliferation of unsecured networks and the unprecedented expectations of users, there is an influx of new device connections as well as a flurry of requests for remote access to sensitive information, as well as the growing threat of spoofing and other web-based threats as users visit rogue websites [17]. In today's world, government agencies in the United States are producing, processing, and

transmitting data at an unparalleled and constantly increasing pace. Although the information technology (IT) environment is continuously evolving, new possibilities and dangers are presented. Agencies throughout the federal government are struggling to stay up with technological advancements.

V. ECONOMIC ADVANTAGES

The rise in employment opportunities for the American market is at the heart of the economic advantages of adding artificial intelligence to IAM. The United States will be necessary to retrain millions of individuals in the United States for them to survive in the workforce. Millions of employees will need help in adapting to the changes brought about by artificial intelligence, robots, and associated technologies. In the field of identity and access management, advancements in automation and Artificial Intelligence (AI) have the potential to bring about levels of prosperity that humans have never before seen. Economic advantages of IAM in the U.S also relate to the development of the Blockchain sector. Since identities may be individually verified in an unchangeable and secure ledger, blockchain technology may be able to address a variety of digital identity issues. Cryptocurrency systems rely on identity verification through public key cryptography-based digital signatures [18]. The sole verification done with this technique is to ensure that the transaction was verified with the proper private key. We deduce that the owner is the individual who has access to the keys. The identity of the owner is irrelevant. Biometrics enhances the capacity to verify a client's identification with a high degree of confidence, enabling automated onboarding and remote access to public services. A variety of biometric technologies are becoming cheaper.

VI. CONCLUSION

This research evaluated how artificial intelligence (AI) is being used in identity and access management, as well as the difficulties that have been encountered and the industry's future. According to the results of this study, continuous authentication ensures that the context of a user is continuously assessed at every contact. AI is capable of analyzing micro-interactions while considering time, location, and even user mobility, and estimating the degree of possible danger at each step along the way. Any future development should incorporate cloud-based integration, as the industry shifts more and more to the cloud. The development of IoT identity and access management is handled via the integration of modern methods. Identity and access management is, therefore, a key component of any business information security because it acts as a barrier between users and sensitive company assets. It contributes to the prevention of stolen usernames and passwords and readily cracked passwords, which are frequent network points of entry for malicious attackers seeking to plant malware or steal data.

REFERENCES

[1] L. Martin, "Identity-based Encryption: From Identity and Access Management to Enterprise Privacy Management", Information Systems Security, vol. 16, no. 1, pp. 9-14, 2007.

[2] J. Singh, "Research Paper on Artificial Intelligence", International Journal of Scientific Research and Management, 2017.

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

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

[5] S. Bandini and S. Manzoni, AI*IA 2005: Advances in Artificial Intelligence. Berlin: Springer, 2005.

[6] S. Bergler, Advances in Artificial Intelligence. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2008.

[7] E. Kldiashvili, Grid technologies for e-Health: applications for telemedicine services and delivery. Hershey, PA: Hershey, PA: Medical Information Science Reference, 2011.

[8] O. Maslak, N. Grishko, K. Vorobiova, O. Hlazunova and M. Maslak, "Developing the intra-firm technology transfer system at the industrial enterprise based on matrix approach", Problems and Perspectives in Management, vol. 15, no. 3, pp. 242-252, 2017.

[9] R. Sharman, S. Smith and M. Gupta, Digital identity and access management. Hershey, PA: Information Science Reference, 2012.

[10] C. Lambrinoudakis, G. Pernul and A. Tjoa, Trust, privacy and security in digital business. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2007.

[11] T. Ryzhakina, N. Koroleva and N. Makasheva, "A process-based approach to management of the enterprise", SHS Web of Conferences, vol. 28, p. 01088, 2016.

[12] B. Wang, D. Liu and M. Ji, "Research on Management System of Mold Manufacturing Enterprise Based on RFID Technology", MATEC Web of Conferences, vol. 95, p. 10002, 2017.

[13] M. Uddin and D. Preston, "Systematic Review of Identity Access Management in Information Security", Journal of Advances in Computer Networks, vol. 3, no. 2, pp. 150-156, 2015.

[14] I. Aguiló, L. Valverde and M. Escrig, Artificial intelligence research and development. Amsterdam: Tokyo, 2003.

[15] R. Lee, Software engineering, artificial intelligence, networking and parallel/distributed computing. Cham : Springer International Publishing : Imprint : Springer, 2015.

[16] S. Phon-Amnuaisuk, S. Ang and S. Lee, Multi-disciplinary Trends in Artificial Intelligence. Cham, Switzerland: Cham, Switzerland : Springer, 2017.

[17] J. Sołdek and L. Drobiazgiewicz, Artificial intelligence and security in computing systems. [Place of publication not identified]: Springer, 2013.

[18] S. Zhong, Proceedings of the 2012 International Conference on Cybernetics and Informatics. New York, NY: Springer New York, 2014.