The Impact of AI on Identity and Access Management: An empirical analysis

Ishaq Azhar Mohammed

Sr. Software Engineer & Department of Information Technology

Hyderabad, India

Abstract*-The main purpose of this paper is to conduct an empirical analysis on how artificial intelligence impacts Identity and Access Management. Artificial Intelligence (AI) and Machine Language (ML) are having a significant effect on the security sector [1]. Developers of identity access management solutions consider these technologies as important opportunity that they should provide to their clients. Artificial intelligence analytics may offer greater perspective and contextual insights, allowing more time-efficient operations for technical and non-technical personnel. Technological advancements offer fresh insights and automated procedures, which dramatically accelerate current IAM compliance checks [2]. They are capable of detecting abnormalities and possible threats without the need for a big security personnel. This provides both specialized and non-specialized employees with the skills they need to take the necessary decisions. Such development is important, particularly in the field of anti-money laundering and fraud detection, as well as in countering malicious attacks. Additionally, it opens the door for the transition from reactive to preventive or even corrective access management. This means that companies are constantly controlled, safe and consistently compliant.*

Keywords: *Artificial intelligence, Identity and Access Management (IAM), Analytics, Automation*

I. INTRODUCTION

People and businesses interact frequently in today's global and highly linked business world. On one side, a firm will become more and more efficient and productive, but on the other hand it is more likely to suffer a compromise of the data or experience another cyber attack.Most companies struggle with choosing who should have access to the database, and ignoring it may leave their systems vulnerable [3]. This is why the value of a well thought-out and mature Identity and Access Management (IAM) strategy cannot be overstated. According to research from analyst firms, more than 70% of businesses do not take IAM seriously. This implies that the danger of data breaches for these companies is twice as great as those that have their IAM Strategy. Research findings also indicate that the more intelligent an IAM method is, the lower the safety risk. Hackers are becoming more skilled and daring in their attempts to infiltrate networks. Detecting unwanted access attempts needs a high level of expertise that human monitoring cannot provide. That's why businesses depend on artificial intelligence technology to adopt better IAM practices to improve access management and protect access control integrity [3, 4]. Whenever AI and machine learning are combined with suitable monitoring and reporting technologies, it becomes feasible to monitor network access and mitigate general breaches exposure via the use of intelligent and adaptive IAM restrictions. When it comes to the highly competitive market of global banking and regulated sectors, investing in artificial intelligence and machine learning will enhance the precision and effectiveness of compliance systems, among other things. As a result, this paper will go into depth on how AI plays a significant role in enhancing identity and access management functions.

II. PROBLEM STATEMENT

The main problem that this paper will solve is to understand how artificial intelligence impact's identity and access management. Due to the worldwide nature of today's corporate environment and its high degree of interconnectedness, the likelihood of a company being a victim of a data breach or similar cyber-attack increases. Companies struggle to decide who should have access to what data, leaving their systems insecure. The reality is that the value of a well-thought-out and sophisticated Identity & Access Management (IAM) strategy cannot be overstated. According to a study published by Forrester, 83% of companies do not have a mature IAM strategy [4]. The danger of these companies facing a data breach is double that of organizations with a mature IAM system. The study also demonstrates a clear connection between intelligent IAM methods and decreased safety risks, better productivity, improved privileged activities and a significant reduction in financial loss over less sophisticated counterparts. One common IAM problem is that users are granted rights of access depending on their management role, although employees seldom perform assigned responsibilities [4]. They may need unique one-time access or every individual who has the same job may need somewhat different access kinds. As a consequence, highly complex situations arise, which often need the cooperation of several departments. Proper management therefore requires the participation of many workers from all levels of the company [5]. This may lead to employees suffering from so-called "safety fatigue" due to a large quantity of technical data, a tough decision-making process and a lack of sensitivity to their daily work. Dreadful repercussions for companies as a result of an inadequately managed IAM system will be just around the horizon.

III. LITERATURE REVIEW

A. Approach to AI in IAM

AI leverages machine learning to provide insights into a business's current identity and access status. Machine learning algorithms are very effective in detecting abnormalities in intelligence work and in establishing a so-called baseline model. This model is converted into rules. Next, these standards are frequently checked in the context of particular audits or news initiatives by the appropriate parties. Any of these parameters, as well as any abnormalities that have been identified in the present state, will be used in the evaluation of all future events [5,6]. Much of the business context and data is not covered by the tools and setup, and therefore cannot be found automatically. Researchers prefer to use machine learning as a virtual assistant alongside an expert, to help dig the evidence, and to identify anything unusual for human evaluation as a baseline and a warning. Such virtual assistant can make it easy to modify the IAM controls more up to speed.

B. How can AI improve effective Identity and access Management

Artificial intelligence technology may be an important aid for successful IAM and can assist prevent many problems. These technologies may help companies to evolve from an excessively technical approach to access management into a type of access management that can be understood at all levels of company [6]. Although in many companies this scenario is very frequent, it doesn't have to be. Artificial intelligence technologies will prove to be very helpful in the implementation of successful IAM and assist prevent a great deal of frustration. These platforms will help companies to develop from an excessively technical approach to access control into a strategy that is comprehensible at every level in an organization. Regardless of the fact that artificial intelligence capabilities have many advantages, many individuals are under the impression that this technology can automate the whole IAM process and eliminate the need for human intervention [6]. This is not the case nowadays. In reality, these contemporary technologies are most helpful when they are used to do a single job rather than many. Although complete automation is not yet feasible, AI and machine learning can certainly assist and enhance the administration of identification and access.

C. Advanced analytics

Artificial intelligence coupled with analytics may offer greater focus and contextual insights, allowing both technical and non-technical workers to perform more efficiently. Modern technologies offer methods of acquiring fresh insights and automating procedures that may dramatically accelerate existing IAM compliance measures. Without the requirement of security specialists, they can identify abnormalities and possible risks [6]. This provides workers the knowledge they need to make the right choices. This is important, especially in the context of the identification of fraud and in the fight against insider threats. This enables companies to be constantly managed, secured and compliant.

• More accurate control of access

As far as biometric passwords are concerned, it is not difficult to imagine AI can identify a person with additional security via sight and sound. Using visual and auditory cues, a computer can identify and validate if a person was who they stated to be, rather than verifying against pre-defined authentication. They can also learn how to give access and take appropriate action. Allowing access based on machine learning is the obvious next step after biometric ID [8]. AI systems that work under user access restrictions may potentially track any odd or inconsistent behavior in real time. They might find out if a person attempts to access a portion of the system that they would not typically access or obtain more information than normal. It was possible to monitor the rhythm of a user's keyboard and mouse motions in order to detect abnormal or unusual patterns. These security rules enable firms to perform their business securely and depend on improved identification and prevention of infringements [8,9].

• Flexibility and automation

Because AI is capable of monitoring minute aspects of user behavior, it is feasible to automate authentication for low-risk access scenarios, relieving the IT staff of some of the work associated with IAM management [9]. Because AI analyzes user activity data, authentication in low-risk access settings may be automated. It may thus load part of the weight of IAM management and prevent users from having "safety fatigue." AI has the ability to examine all the parameters behind requests for access, including time, device type, location and resources. By taking these considerations into account before providing network access, IAM becomes contextual and granular, and it is possible to control potential issues caused by incorrect provisioning or deprovisioning. AI-powered systems are capable of applying suitable IAM rules to every access token depending on the user's requirements and conditions, saving the IT staff time spent working out the fundamentals of "least privilege" for each use case or addressing privilege creep issues.

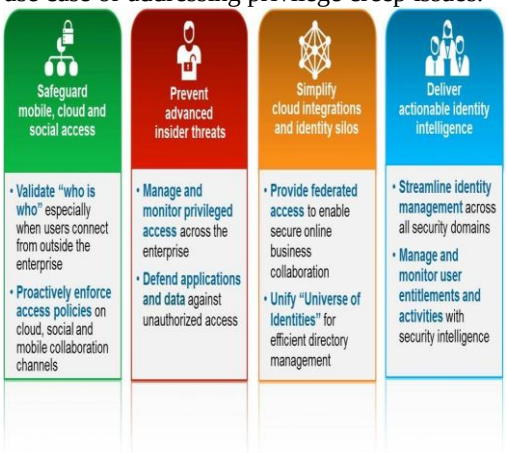

Fig i: A threat-aware identity and access management

- ***Going Above and Beyond Compliance***

Many businesses believe that adhering to security and privacy laws is good enough to keep cybercriminals at bay. Indeed, these regulations are insufficient to satisfy the security requirements of any business [9]. The fundamentals of compliance include limiting access to information from those who need it and disregarding everyone else. The adaptability and flexibility of AI-powered IAM is very beneficial in these circumstances. Due to the fact that AI and machine learning are continuously monitoring traffic, learning habits, and enforcing security rules, businesses have less challenges implementing security standards, and it becomes more difficult for hackers to use stolen credentials [9].

AI is no longer a novel concept that no one can execute practically. It has developed into a trend in today's cyber security setting. The high level of interconnection, the growing number of human and device identities, as well as the widespread practice of worldwide access will compel businesses to integrate smarter technology into their security procedures. Additionally, businesses will need sophisticated identity intelligence driven by artificial intelligence to adopt a risk-based strategy to Identity and Access Management (IAM) [10]. Industry best practices have shown that machine learning-based identity analytics significantly improves IAM design and program management.

Enterprise software solutions that include artificial intelligence may significantly 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 capable of keeping hackers at bay, but this is not the case [10]. Compliance at its most fundamental level is limiting access to the information to those who require it and denying everyone else. Complying with new security regulations may be a hardship, and disobedience is a frequent occurrence. The adaptability and flexibility of AI-powered IAM is advantageous in these circumstances [11]. AI and machine learning continuously monitor traffic, understand user behaviors, and apply precise access restrictions, easing the burden on businesses to enforce security procedures and making it very difficult for attackers to exploit stolen information.

D. Elimity's approach to artificial intelligence in IAM

Elimity leverages machine learning to provide perspectives into a business's current identification and accessibility configuration. Algorithms are adept at identifying outliers and helping in the establishment of a so-called baseline model [12]. This model is converted into Elimity rules. Then, in the context of particular audits or

reporting activities, such rules may be validated by the relevant individuals. If necessary, the rules may be modified to more closely match the actual situation inside the company and to account for the business environment. Any of these guidelines, as well as any abnormalities found in the present condition, will be utilized to evaluate all future reporting. This is not a big bang approach to artificial intelligence [12]. A significant amount of corporate environment and information is not covered by the tools and setup, and therefore cannot be found automatically. We are a firm believer in AI's additive role: we use machine learning as a virtual assistant alongside an expert to aid in digging through data, determining what is normal, and flagging anything out of the ordinary for human assessment [13,14]. This virtual assistant will aid in automating IAM controls in order to maintain a more continuous state of control.

IV. FUTURE IN THE U.S.

While identity management and access control have often been mutually exclusive, AI will serve as the glue that binds them together in the future with greater impact experience in United States. Advancing beyond biometric authentication, it's not hard to envisage AI detecting a person with additional security using sight and voice. Instead of verifying against pre-defined credentials, a computer might comprehend and authenticate a person's identity using visual and auditory cues [15]. Additionally, it may learn when to give access and respond appropriately. Allowing access based on machine learning is a natural development from the biometric identification. Although this is a revolutionary innovation, biometrics still pose risks. This implies that since the majority of people's smartphones now generate such precise pictures, those who post peace sign selfies on social media pages may unintentionally provide prospective cybercriminals with their fingerprints. AI also has the ability to provide intelligent, real-time security, allowing for the implementation of fine-grained access control. AI algorithms may track users' activities around the internet. However, behavioral variables and real-time risk assessments may also be involved.

Within the confines of a user's user privileges, AI systems might monitor any odd, illogical, or unpredictable behavior in real time. They might determine if a person is attempting to access a section of the system that they would not usually access or download more files than they would usually. It will be possible to monitor the rhythm of a user's keyboard and mouse strokes in order to detect abnormal or unusual behavior patterns [15,16]. Furthermore, information from an individual's internet-based identification and behavior - their online profile, organizations they belong to, people they follow, and sites they frequent – may be utilized to establish a risk score. After putting all of this information together, the AI system may take a variety of measures, ranging from sending a warning to a user to turning off particular parts of a corporate system for that user to denying them access to a system entirely [17]. Naturally, with this degree of surveillance, privacy issues arise, creating a whole new area of debate. It is certain that the genuinely intelligent system of the future will be capable of knowing, comprehending, monitoring, and acting, while eliciting whatever information it needs from the user 17,18]. Identity and credentials will not exist in isolation. The identity of a person will serve as their credentials. Any artificial intelligence system will strive to achieve this as its ultimate objective.

V. ECONOMIC BENEFITS

Artificial intelligence (AI) has the potential to revolutionize US commerce. Specific applications in fields such as big data and translation services are already eliminating trade barriers. Artificial intelligence is already influencing the creation and administration of global value chains. It may be used to enhance forecasts of future trends, such as shifts in consumer demand, and to handle risk more effectively across the supply chain. By enabling businesses to manage complex and distant manufacturing units more effectively, such technologies increase the overall productivity of GVCs [19,20]. For instance, businesses in the United States may utilize AI to enhance warehousing, demand forecasting, and just-in-time production and delivery accuracy. Robotics can improve packaging and inventory monitoring efficiency and productivity. Additionally, businesses may use AI to enhance physical inspection and upkeep of assets across supply chains. Additionally, AI has the ability to enhance the results of international trade talks [20]. For example, AI could be used to improve the analysis of each negotiating partner's economic trajectory under a variety of different assumptions, such as outcome measures contingent on trade negotiations (economic expansion mechanisms under various tariffs or quotas on imports), how these outputs are impacted in a multiplayer situation in which import tariffs are reduced at varying rates, and forecasting the trade response.

VI. CONCLUSION

This study addressed how artificial intelligence impacts identity and access management. The purpose of this research was to examine the effect of artificial intelligence on identification and access management. It is becoming increasingly evident that artificial intelligence (AI) will play a significant role in cybersecurity and identity and access management. Many companies, however, are unsure how AI might be used to enhance their IAM process. These results from this study show that the amount of end utilities and customers that use various applications and platforms from numerous devices rises as a business evolves. It is frequently not the management of identification that is the reason for data infringements, but the transfer of identities to an unknown person. While the restriction of privilege access provides some security, it is obvious that there are deficiencies. Businesses are already using these pattern-matching skills in a variety of applications. The machine learning program recognizes images and recognizes voice. It is granting loans based on customer behavior patterns and assisting in the detection of financial misconduct. These algorithms' features correspond well to the IAM issue. An artificial intelligence tool will analyze previous access data from an identity and access management systems, including who visited an application, when they visited it, and from where they viewed it. Information such as what they explicitly sought access to and from which device may also be useful in refining these models, as may be provided by various sources. Similarly, to how machine learning algorithms will study how a face appears, they will also master what typical access patterns appears.

REFERENCES

[1] V. Dimitrova, Artificial intelligence in education: building learning systems that care: from knowledge representation to affective modelling. Amsterdam: IOS Press, 2009.

[2] 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.

[3] M. Maula, Organizations as learning systems. Amsterdam: Elsevier, 2006.

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

[5] A. Morgans and F. Archer, "Impact of Rural Identity on Access to Emergency Health Care for Asthma: Impact of Community Perceptions", Prehospital and Disaster Medicine, vol. 20, no. 2, pp. S140-S140, 2005.

[6] 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.

[7] R. Nkambou, J. Bourdeau and R. Mizoguchi, Advances in Intelligent Tutoring Systems. Berlin: Springer Berlin Heidelberg, 2010.

[8] T. Osmanoglu, Identity and access management: business performance through connected intelligence. Waltham, MA: Syngress, 2014.

[9] E. Damiani, S. De Capitani diVimercati and P. Samarati, "Managing multiple and dependable identities", IEEE Internet Computing, vol. 7, no. 6, pp. 29-37, 2003.

[10] C. Sennewald, Effective Security Management (Fifth Edition). Butterworth-Heinemann, 2011.

[11] K. Flieder, "Identity- und Access-Management mit EAI-Konzepten und -Technologien", Datenschutz und Datensicherheit - DuD, vol. 32, no. 8, pp. 532-536, 2008.

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

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

[14] G. Goth, "Identity management, access specs are rolling along", IEEE Internet Computing, vol. 9, no. 1, pp. 9-11, 2005.

[15] L. Iliadis, I. Maglogiannis and H. Papadopoulos, Artificial intelligence applications and innovations. Heidelberg: Springer, 2012.

[16] H. Sasaki, Intelligent and knowledge-based computing for business and organizational advancements. Hershey, PA: Information Science Reference, 2012.J. Sołdek and L. Drobiazgiewicz, Artificial Intelligence and Security in Computing Systems. Boston: Springer US, 2003.

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

[18] T. Martens, "Electronic identity management in Estonia between market and state governance", Identity in the Information Society, vol. 3, no. 1, pp. 213-233, 2010.

[19] J. A. Zachman, “A framework for information systems architecture,” IBM Syst. J., vol. 26, no. 3, pp. 276–292, 1987.

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