Artificial Intelligence: The Key to Self-Driving Identity Governance

Ishaq Azhar Mohammed

Data Scientist & Department of Information Technology

Dubai, UAE

Abstract*-The main goal of this article is to examine how artificial intelligence is playing an increasingly important role in advancing identity governance. The speed of global digital change is accelerating, and businesses are under increasing pressure to guarantee that their technology can keep up with the times. Today's headlines often include stories about high-profile data leakage, which have a significant impact on a company's image and financial health [1]. The moment has come for businesses to invest in AI-powered identity security to remain abreast of security and compliance risks. Information technology, a shifting workforce, and an onslaught of compliance regulations have brought an unprecedented number of users, points of access, apps, and data, to the point that IT departments are struggling to stay up [1]. A human-centric approach to identity security can only scale so far, and with it comes inaccuracy in risk identification. Security requirements are becoming more complicated, decentralized, and integrated with business operations, owing to new methods of working enabled by cloud technology [2]. This implies that robust identity governance and access control are more critical than ever. In this paper, we examine the current status of the information technology environment and explain how artificial intelligence will help companies address their present issues relating to identity governance.*

Keywords: *Artificial intelligence, identity governance, cybersecurity, automation, identities, self-driving identity*

I. INTRODUCTION

A new generation of identification powered by AI is required. This allows identification to be independent while being fully controlled like SailPoint Identity Platform. SailPoint Identity Platform leverages the power of AI and machine learning to help businesses stay on top of the security curve by proactively identifying problematic individuals and access that may represent a concern [2]. It evolves and adjusts to the changing needs of the business, allowing administrators to guarantee that every user gets the access they need when they want it. It maintains and monitors all of the organizations' access. Essentially, it simplifies the process of establishing identification. Identity governance has become a key component of the identity and access management initiatives of the majority of businesses. It enables companies to offer secure automated access to digital assets while also minimizing compliance concerns [3]. When it comes to identity governance, one of the most difficult issues is defining and managing roles and rules that assist simplify and manage access assignments, particularly in big organizations with numerous different systems [3]. These difficulties may be substantially mitigated by using artificial intelligence (AI) principles. This paper will discuss the value that artificial intelligence may provide to Identity Governance systems and what we can anticipate from technology companies that specialize in this area.

II. PROBLEM STATEMENT

The main problem this paper address is the use of artificial intelligence for self-driving identity governance. The mixed IT systems of today may make it difficult to implement comprehensive identity governance. Businesses must safeguard customer data, proprietary information, financial data, and other sensitive information from breaches and illegal access. Because data may be accessible by people, processes, and technology, businesses must take a multi-pronged strategy to data protection. A critical first step is to establish a strong governance structure for identity access and management [4]. This should be comprehensive across all of the business assets: cloud applications, on-premise software solutions, database systems, and line-of-business applications. Businesses use many security precautions to safeguard their systems, but the critical component of data protection is the establishment of appropriate identity access management and access control mechanisms [5]. The primary issue with the access control and entitlements performance review is ensuring that user access privileges and entitlements are reviewed continually. Access reviews are a time-consuming, laborious, and tedious process that involves identifying users, entitlements, and supervisors for ongoing evaluation.

III. LITERATURE REVIEW

A. The Rise of Self-Driving Identity Governance

Experts in security and risk management acknowledge that we are living in fascinating and perilous times. The digital revolution is no longer a far-fetched fantasy. Organizations are accelerating their efforts to automate laborious operations, enhance automation, and use large amounts of data to boost efficiency [5]. Each technology that allows digital transformation needs a clear identification of the people who require access, the resources they require, and how access may be managed to avoid illegal use [5]. Simultaneously, cloud apps and services are rapidly gaining traction: 94 percent of companies already utilize some kind of cloud computing. App proliferation is not confined to the cloud [5]. Additionally, the use of DevOps and agile methods make a positive contribution, and each mobile development may have its own organizational culture and entitlements [6]. All of this must be controlled and monitored - a responsibility that rests squarely on the shoulders of security and risk teams. There is positive news, despite these pressures. The revolution is now in terms of identity governance. Hyper-automation and self-driving governance are expected to affect the same magnitude as agile development. As a result, regulatory compliance is accelerated, expenses are lowered, and risk is significantly minimized.

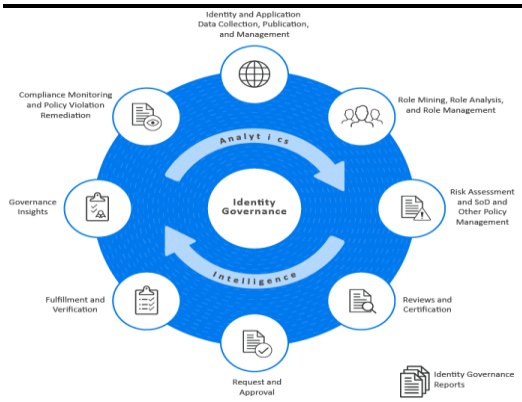

Fig i: Identity Governance in the context of a self-driving service user

B. The Explosion of Identity

Numerous technological and business trends support the growth of identities requiring management: digital revolution; accelerating applications proliferation; the development of DevOps identities; the usage of industrial robot, machine, and device identities; as well as outsourcing operations to third parties. It's just a matter of time until an organization recognizes that handling so many identities, roles, and entitlements is a significant challenge [6]. This issue of "identity explosion" puts a significant load on identity & access personnel, as they must guarantee that each identity only has the accessing rights and protections it requires. Lacking enterprise-wide insight into the identity landscape or contextual information about access permissions and certifications, organizations often get overwhelmed [7]. As a consequence, they wind up rubber-stamping access and certification requests. They just lack the time required to examine each request and decide whether it is essential.

C. Increased Regulatory Compliance Obligations

The job of security and risk teams is made much more complex by a hodgepodge of government and industry laws, including FISMA, SOX, HIPAA, GDPR, and the CCPA [8]. To guard against internal and external cyberattacks that may result in massive breaches, these rules typically require limiting access privileges to those that are the bare minimum required to fulfill job duties - the concept of "least privilege. The proliferation of identities complicates ensuring the least privilege, much more so now, when many workers work remotely, often on personal devices with weak security protections. This undoubtedly affects security compliance - particularly in terms of expenses, which may be very high. GDPR, for instance, costs the typical Fortune 500 business $16 million a year and applies to organizations both within and outside the EU [9]. Penalties for noncompliance with regulatory requirements are similarly severe. A multinational insurance company was recently fined $10 million for non-compliance with SOX rules aimed at ensuring client identification. The US Department of Health and Human Services penalized a Tennessee-based management firm $2.3 million last year during a HIPAA compliance assessment for a compromise triggered by stolen administrative privileges. At a time when companies are under an increasing financial strain, a lack of knowledge of user access and the rationale for its usage may be expensive.

D. Identity Governance Fatigue Sets In

Identity governance and administration (IGA) solutions have long been utilized by security and IT experts to meet user provisioning and regulatory compliance needs. These solutions were created to streamline the process of submitting access requests, obtaining permissions, and conducting certification reviews. The sheer volume of such queries now exceeds the capability of many conventional IGA systems [10]. Teams confronted with a seemingly insurmountable job usually succumb to identity governance fatigue. They are expected to make fast, educated judgments on identity access in situations when a mistake may have severe consequences for the business [11]. Fatigue associated with identity governance leads to inefficiency, delayed reaction times, and poor decision-making, all of which may result in mistakes. Unsurprisingly, companies are interested in automating identity governance solutions.

E. Automated Identity Governance Overcomes Fatigue

Identity and risk specialists fatigued with IDG handle an excessive amount of identities, roles, and rights. The technology and internet of things (IoT) are also proliferating, as well as organizational transformation requirements and the additional effect of unexpected occurrences. To replace outdated manual labor, new automated, self-driving methods are required. Automated identity governance is the best option because it offers an excellent domain for reaping the advantages of automated intelligence and learning techniques [11]. Automation simplifies the intelligence and makes sense of the mass of unrelated data produced regularly. It identifies abnormal activity before it becomes a problem and allows solutions to proactively detect and highlight access concerns and excessive rights. Artificial intelligence (AI) is used to provide intelligent suggestions to policymakers.

There is more to an optimal IGA automation system than just that. It then automatically implements the suggestions, allowing security personnel to devote their attention to more difficult activities, such as researching high-level risks that need the use of highly experienced human involvement. Automating the process of proposing low-risk accounts for certification and re-certifying high-risk accounts may also be very beneficial [12]. AI-based solutions will allow better, more efficient certification campaigns with fully defined access permissions by combining machine learning and artificial intelligence.

F. Using artificial intelligence to support identity governance

In recent years, the software industry has emphasized the use of artificial intelligence (AI), and the security business – particularly the identity governance and administration (IGA) sector – has followed suit. So the issue becomes less about whether a piece of software is AI-enabled and more about what value it is delivering to companies. Consider the concept of compliance. Enterprises today must guarantee that people have adequate access to the relevant apps and that limits are applied when necessary [13,14]. IGA solutions do this, and they can use artificial intelligence to streamline the process. However, the quality of the findings is dependent on the quality of the data, and if there are organizational silos that prohibit IT, teams, from understanding the entire extent of access and privileges, artificial intelligence will be of little use. The following are the reasons: Any IGA solution may identify a user who has an excessive amount of access to information that they do not need or should not have. However, this is just the first part of the fight. It will not be able to offer insight into possible risks connected with access unless it is coherent, company-wide data accessible, and AI and machine learning technologies available to analyze it. What good is it if we don't have a clear view of where these problems are coming from - whether they are caused by outdated IT rules or undiscovered security risks – right? Enterprises must find a method to connect siloed data from throughout their company to avoid this destiny and get the best potential outcomes. When it comes to responding to threats, manual procedures and poorly connected business systems are becoming more inconvenient for businesses. To address this, automating identity governance systems has become a fantastic first step. Using automation to its full

potential may aid in compliance efforts while also allowing managers to get insight into and control over the degrees of access that are most suitable for certain individuals and groups within a business [15].

When these provisions are in effect, IGA technologies can give a comprehensive picture of who has accessibility to what and then use artificial intelligence to automatically approve everything that seems to be in order and flag anything that appears to be incorrect. Not only does this assist in compliance and cybersecurity, but it also saves a significant amount of time. As opposed to reviewing thousands of user access, managers only have to evaluate a portion of them, allowing them to do their tasks faster and more effectively. This is one of the reasons why many companies rely on IT Service Management (ITSM) systems to manage their IGA initiatives, to some extent. Integrating these capabilities into an organization's current systems allows IT teams to view the entire spectrum of identity and accessibility in the context of all business systems, which saves time and money. When this is the case, artificial intelligence may be applied to a greater number of use cases, resulting in superior outcomes. It not only helps to enhance the overall IGA and security of a company, but it also has implications for security operations (SecOps), governance, risk management, and compliance (GRC), as well as incident response procedures [15]. For example, IGA can check that active GRC controls are in place during access review and process approval, and it may identify which rules may conflict with a particular authorization. It may automate the gathering of evidence that users are complying to control rules and decide if additional analysis is required for auditing purposes by analyzing the evidence collected. In addition, AI enablement may assist in the correlation of access requests with change control items, ensuring that access changes are not made in advance of system updates that would make the access change ineffective or obsolete. Furthermore, IGA powered by AI may connect user access with known security issues or exploits that exist on the system that the requester is using to make the request. In the case that a user's computer is hacked, this allows SecOps to get insight into rights on the infected system. This also allows for the instant suspension of all account rights, which may prevent a breach from propagating to other computers in the future. This is very beneficial since, when it comes to threat protection, speed is of importance. While improved GRC and SecOps procedures are some of the beneficial consequences of an AI-driven IGA program, the true value lies in the fact that it enables companies to adopt a proactive approach to identity management. As opposed to maintaining an overly defensive posture in terms of security and compliance, or jumping from one crisis to another, teams may use the data they currently have to make educated choices and act to avoid issues from arising in the first place [16].

IV. FUTURE IN THE U.S

In the United States, the shift to a digital era has already started and is progressing rapidly. Artificial intelligence research and development (AI R&D) is a key priority for the United States and has received widespread bipartisan support. Artificial intelligence (AI) is posing new problems and placing pressure on public entities to adapt. Governments and companies are increasingly relying on algorithms for decision-making [16,17]. They are transforming employment through the use of automated evaluation tools, assisting in the provision of government services, streamlining government procedures, altering the way criminal justice works through the use of predictive policing, and reshaping educational systems through the use of automatic evaluation tools. However, many of these advances are characterized by low levels of openness and public awareness, as well as a lack of oversight mechanisms. The dangers associated with this transformation are equally significant, presenting significant governance difficulties. The American AI Initiatives calls for all administrative government departments that are involved in the development or deployment of artificial intelligence, giving educational funding, or regulating or directing to adhere to six strategic goals to be successful [18]. This includes promoting sustained investment in artificial intelligence research and development; increasing access to Federal data, prototypes, and computational resources; reducing obstacles to using Artificial intelligence; making sure that performance standards significantly reduce security vulnerabilities to attacks from cybercriminals; training American artificial intelligence scientists, and instituting an intervention plan to protect the United States' economic and national security (in a nutshell). The chiefs of each agency are being asked to raise their attention and funding for artificial intelligence (AI) in the next fiscal year and every year after that.

V. ECONOMIC GAINS

If artificial intelligence is used to self-driving identity governance in the United States, the economic advantages may be realized gradually and become apparent over time. The effect of artificial intelligence may not be linear but rather may accumulate at an increasing rate over time. By 2030, artificial intelligence's contribution to growth maybe three or more times greater than it is during the following five years. Increasing external and internal cyber threats need security and risk professionals to work smarter rather than harder to successfully defend the company from these dangers [19]. This simply implies that old identity, governance, and infrastructure procedures and solutions must be significantly improved, not just in terms of functionality, but also in terms of their ability to provide commercial value. To maximize the business value of their legacy identity, governance, and infrastructure solutions, enterprises must adopt a proactive approach to implementing an AI-driven analytics solution that provides contextual enterprise-wide risk awareness, strengthened business performance, and speeded up decision-making. Throughout the past decade, artificial intelligence (AI) applications have grown more common, revolutionizing the way we operate, play, and connect and the rest of the world. Increasingly, artificial intelligence (AI) is being woven into the fabric of corporate operations and is being extensively implemented across a wide range of application use cases [19]. Not all industries, however, have reached the same level of sophistication: the information technology and telecommunications sector are the most advanced in terms of AI adoption, with the automobile industry trailing close behind. According to a recent worldwide study that surveyed more than 4,500 technology decision-makers from a variety of industries, 45 percent of big businesses and 29 percent of SMEs said that they have used artificial intelligence technologies. As cyber threats become more sophisticated, artificial intelligence (AI) will become more important in the cybersecurity business. Indeed, the global cybersecurity industry is predicted to expand and create more opportunities for employment. More technological devices utilizing AI will be needed and therefore will boost the manufacturing and IT industry in the United States. The use of artificial intelligence (AI) is not without dangers, however, as more than 60% of businesses that have adopted AI consider cybersecurity threats created by AI to be the most significant.

VI. CONCLUSION

This study investigated how artificial intelligence is altering the self-driving identity governance system. According to the findings of this study, the automation that originates from a next-generation, AI-driven identity governance program penetrates many areas of an organization and has a broad impact. Identity governance and a global cybersecurity strategy can assist preserve and even consolidate brand reputation in their capacity to regulate access across a complex identity environment, which helps protect businesses from various cyber threats and reduces risks. To produce educated suggestions that can be conveyed to decision-makers, artificial intelligence (AI) is employed. There is more to an optimal IGA automation system than just that. It then automatically implements the suggestions, allowing security personnel to devote their attention to more difficult activities, such as researching high-level risks that need the use of highly experienced human involvement. Automating the process of proposing low-risk accounts for certifications and re-certifying high-risk accounts may also be very beneficial. A system based on artificial intelligence will allow more optimized and efficient certification initiatives with fully defined access permissions.

REFERENCES

[1] M. Gupta, J. Walp, and R. Sharman, Strategic and Practical Approaches for Information Security Governance: Tchnologies and Applied Solutions. Hershey, PA.: Information Science Reference, 2012.

[2] M. Hildebrandt, Digital Enlightenment Yearbook 2013: the Value of Personal Data. Amsterdam: IOS Press, 2013.

[3] D. Hutchison, E. Ferro, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. P. Rangan, H. J. Scholl, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, and M. A. Wimmer, Electronic Government 7th International Conference, EGOV 2008, Turin, Italy, August 31 - September 5, 2008. Proceedings. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2008.

[4] E. Kajan, Electronic business interoperability: concepts, opportunities and challenges. Hershey, PA: Business Science Reference, 2011.

[5] Z. Mahmood, Emerging mobile and Web 2.0 technologies for connected e-government. Hershey, PA: Information Science Reference, 2014.

[6] R. Meersman, On the move to meaningful internet systems: OTM 2011: Confederated International Conferences: CoopIS, DOA-SVI, and ODBASE 2011, Hersonissos, Crete, Greece, October 17-21, 2011, proceedings. Berlin: Springer, 2011.

[7] S. Sandri, Marrè Miquel Sànchez i, and Cortés Ulises, Artificial intelligence research and development: proceedings of the 12th International Conference of the Catalan Association for Artificial Intelligence. Amsterdam: IOS Press, 2009.

[8] M. Schultz, S. A. Maguire, and A. Langley, Constructing identity in and around organizations. Oxford: Oxford Univ. Press, 2013.

[9] J. J. Zaaiman and L. Leenen, Proceedings of the 10th International Conference on Cyber Warfare and Security, ICCWS-2015: co-hosted by the University of Venda and the Council for Scientific and Industrial Research, Kruger National Park, South Africa 24-25 March, 2015. Reading, UK: Academic Conferences and Publishing International Limited, 2015.

[10] Fischer-Hübner Simone, L. Fritsch, and E. de Leeuw, Policies and research in identity management: second IFIP WG 11.6 working conference, IDMAN 2010, Oslo, Norway, November 18-19, 2010; proceedings. Berlin: Springer, 2010.

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

[12] C. N. Silva, Citizen e-participation in urban governance: crowdsourcing and collaborative creativity. Hershey, PA: Information Science Reference, 2013.

[13] M. Rijal and S. G. Pradhan, Readings on governance and development. Kathmandu: Institute of Governance and Development, 2002.

[14] M. van Essen, P. Engelen and M. Carney, "Does “Good” Corporate Governance Help in a Crisis? The Impact of Country- and Firm-Level Governance Mechanisms in the European Financial Crisis", Corporate Governance: An International Review, vol. 21, no. 3, pp. 201-224, 2012.

[15] T. E. Osmanoglu, Identity and access management: controlling your network. Rockland, MA: Syngress, 2014.

[16] M. Gurstein, "Social impacts of selected artificial intelligence applications", Futures, vol. 17, no. 6, pp. 652-671, 1985.

[17] E. Bertino and K. Takahashi, Identity management concepts, technologies, and systems. Boston, MA: ARTECH, 2011.

[18] Bücker Axel, Identity management design guide with IBM Tivoli identity manager. Poughkeepsie, NY: IBM International Technical Support Organization, 2009.

[19] J. Camenisch, Fischer-Hübner Simone, and K. Rannenberg, Privacy and Identity Management for Life. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.