IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A significance of Identity Management as a Prerequisite for Enterprise AI on the Cloud

Ishaq Azhar Mohammed

Sr. Data Scientist & Department of Information Technology

Dubai, UAE

Abstract-*This paper provides a review on the significance of identity management for enterprise AI on the cloud. In addition to data security and authentication, identity management is continuously developing across key tasks such as synchronizing internal data, allowing consumer contact preference management, and fulfilling privacy compliance needs, to mention a few [1]. Protection of corporate information systems from data breaches, hostile insiders, and fraud continues to be a key business concern, and this is fueling the need for better identity analytics that can dynamically identify abnormal user behavior [1]. IT professionals' work is becoming somewhat simpler as identity and access management solutions grow more automated — but they can't fully delegate their responsibilities just yet. Many innovations in the identity and access management (IAM) sector have been driven by mobile technology in recent years, with suppliers being encouraged to enhance usability on mobile devices as a result. Identity and access management solutions are now being enhanced by the incorporation of advancements like artificial intelligence, machine learning, microservices, and cloud services, often with the idea of achieving them more smooth, accessible, and automated for both end-users and IT [2].*

Keywords: *Identity and access management, artificial intelligence, biometrics, IAM systems, identity management*

I. INTRODUCTION

Why has business artificial intelligence in the cloud come to a halt? For the most part, this is due to legitimate security concerns. Furthermore, AI's insatiable hunger for data — most of it sensitive — has resulted in significant clashes with the security posture of organizations [3]. However, the march of artificial intelligence and machine learning into the cloud seems to be unavoidable. Some businesses turn to the past for inspiration. However, previous security methods, it seems, are not particularly effective at present. Recent stories about the data leak at Capital One (and other companies) seem to have strengthened this argument. In this post, I will discuss the important factors for identity-based security that are required to offer a safe basis for business artificial intelligence (AI) on the cloud. The mitigation of security barriers to AI adoption may be accomplished by resolving these issues, allowing businesses to once again accelerate the use of AI [3].

The main objective of identity management in cloud computing is to manage personal identification information to ensure that access to computer resources, applications, data, and services is appropriately managed and monitored [4]. IT identity management is the only area of information technology security that provides real advantages in addition to minimizing the risk of security breaches. Identity management aids in the prevention of security breaches and plays an important role in assisting your business in meeting IT security requirements. When it comes to protecting the financial data of your customers or your business against illegal access, the advantages may be enormous. In addition, you gain many advantages from identity management that takes place daily rather than just when a significant danger is present [5]. The precision and speed of digital identification access rights in near real-time have been improved by a next-generation intelligent system. The patent-pending IAM feature, which aggregates data from various systems and sources, reduces the complexity of controlling and monitoring who has access to what information and resources. By using artificial intelligence and machine learning to contextualize identification choices and constantly keep up with ever-shifting modifications to user access rights, it enhances the accuracy as well as the speed at which near real-time adjustments to user privileges are made. This will assist businesses in proactively identifying higher-risk regions that may need more governance, thus eliminating the requirement for error-prone manual provisioning techniques that are currently used by today's identity and access management systems [6]. Provisioning of access to users should be based on a clear understanding of who the individual is and why they need the access.

When it comes to managing user rights, this should be the case. Because current methods to access control are based on educated guesses rather than comprehensive facts, they provide a significant problem. With our identity and access management capabilities, we've developed a proactive approach to identity management that helps minimize human error and expense while also improving risk awareness and making outliers simpler to detect [7]. Swinging doors and turnstiles benefit from integrated systems that include sophisticated analytics and artificial intelligence (AI). These solutions provide increased functionality while also improving security. While artificial intelligence is becoming more important in a wide range of company operations in a wide range of market sectors across the world, security applications have been slower to incorporate it into their

operations. Nonetheless, the increased health hazards that businesses are now exposed to have compelled both security solution providers and end-users to reconsider how artificial intelligence might assist reduce those risks [8]. There is no doubt that artificial intelligence can significantly improve the security of external and interior entrances if it is used in the near term during this crisis to achieve this goal. Even though AI can assist with many security-related tasks, such as distinguishing people from objects at a facility's perimeter and interior entrances, detecting attempts to piggyback on other people, spotting and analyzing potentially lethal objects and dangerous people, among other things, AI analytics cannot prevent unauthorized human entry or deny the entry of dangerous objects [9]. The purpose of this article is to examine how identity management is a requirement for business artificial intelligence and cloud computing.

II. PROBLEM STATEMENT

The main problem that this paper will try to solve is to review how identity management is a prerequisite of enterprise artificial intelligence and cloud. Cybercriminals are becoming more aware of the techniques used by businesses to protect their networks, and they are developing more subtle means of entering networks. To detect illegal access attempts, meticulous inspection is required, something that human monitoring is no longer capable of providing [10]. Because of this, organizations are turning to artificial intelligence (AI) technology, such as machine learning (ML), to adopt better identity and access management (IAM) practices, to increase access security while preserving the integrity of user identities. AI is no longer a nebulous, future concept that no one can practically apply, but 83 percent of companies have not yet matured in their approach to information and asset management [12]. Businesses must begin to integrate smarter technology into their security procedures as a result of increased interconnectedness, an increase in the number of human and device identities, and the trend toward worldwide access. When artificial intelligence and machine learning (AI and ML) are combined with suitable monitoring and reporting technologies, it becomes possible to visualize network access and decrease total breach risk by implementing intelligent, adaptive identity and access management rules.

III. LITERATURE REVIEW

A. *Traditional Techniques for Cloud*

Historically, the main focus of corporate security was on protecting the network perimeter. Essentially, the aim was to create an impenetrable network barrier around the centralized server based on the assumption that a secure network perimeter ensures that all systems, data, and resources inside the data center are safe and reliable [12]. When this was done, it made sense since the vast majority of applications and assets resided or cooperated almost entirely inside the data center, making the process of developing, operating, and managing security applications and assets simpler. Earlier methods for protecting legacy data centers were shown to be predicated on a fundamentally faulty premise, which is that the network perimeter is secure [12]. Unfortunately, this has resulted in older techniques for protecting legacy data centers being rendered ineffective. However, when applied to the cloud, this is a faulty sound assumption for a variety of reasons. For starters, today's adversaries are more intelligent and have access to better technologies, leading network perimeters to seem to grow more permeable [13]. Uber's latest data leak on the cloud showed unequivocally that this is the case, as well.

The second instance in which mistakes will be committed is when businesses protect their cloud tenancy. Unfortunately, all it takes is a single configuration change for one endpoint to be compromised, enabling an adversary to rapidly establish a foothold over an extensive swath of the whole network. And I would argue that entropy alone — the fact that security settings unavoidably drift over time — is a sufficient reason to be wary of a network-based security barrier in the first place. Capital One's recent cloud computing experience may be the most poignant illustration of this phenomenon [13].

Finally, the very nature of the cloud presents a security issue: by default, many resources are intended to be available through the internet at the time of their production, posing a risk to users' personal information. This adds a new degree of complexity, which provides security for all cloud components, for which most companies are not prepared [13]. And all it takes is a mistake to trigger a potentially catastrophic data violation. Indeed, it is so large that I think it is reasonable to argue that contemporary cloud security methods should now be explicitly supposed to break the network perimeter. AI practitioners – data scientists — still need large quantities of sensitive data, exacerbating the problem. It is very real security concerns that enable enormous quantities of sensitive data to remain in the cloud [14].

B. *Enterprise Demands have Driven AI Cloud Adoption*

Today, AI is driving the need for a new approach to business data—which enables data quantities of scale that are greater than those of traditional transaction systems. Furthermore, the scalability requirements to analyze and train this amount of data have pushed companies to relocate out of the security of their relatively safe data centers [14]. Only the main cloud platforms can now offer the cost-efficient, on-demand, and scalable GPU base that contemporary AI needs.

C. Identity as a New Security Perimeter

Identity has now become the new border of security. Simply put, identity-based security guarantees that you are who we say you are and that you can only do what you can – no matter where you are and no matter how you access your information. Identification-based security says that your identity — or your ID credentials — includes the methods for authentication (who you are) and information about your permits (what you can do). In particular, proper credentials provided by one's identity are required for access to any interface, services, or resources or to access any data [15].

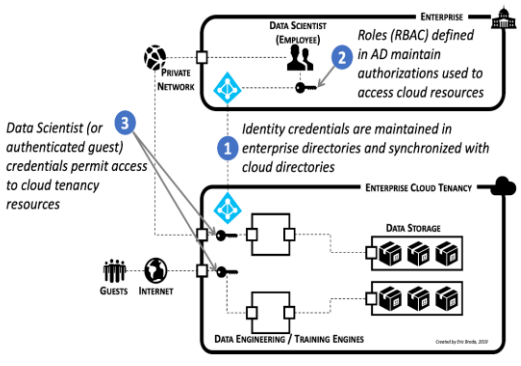

Fig i: Process of enterprise AI in cloud

D. *Integrated Identity Management is Critical*

So how should identities be handled when identities become the focus of cloud tenancy security? Here are some important factors for the cloud tenancy of a company. Delay, on-prem, and cloud directories must be synced (for instance: Microsoft Active Directory or LDAP). It enables the uniform management of identities and related credentials, irrespective of where the identity is generated or used [16,17]. From the viewpoint of data scientists, this is the foundation for an identity-based strategy for the securement of critical AI data and a simple single sign-on process to connect to the cloud

and on-site systems in managing multiple IDs and passwords. Secondly, the on-prem instance is the master that offers a single authoritative identity source. This simplifies identity management procedures and also reduces safety concerns because of human mistakes and configuration complexity.

E. Role-Based Access Control (RBAC)

RBAC is a method for ruling authorizations or role-based access control. Roles are usually kept in the ID directory of a company (Active Directory, for example). These roles are utilized for resource access [17]. RBAC operates like this (albeit it's simplified): Roles are often established to reflect job functions; roles are allowed for different activities. Then users/employees are usually allocated to groups that are then given responsibilities in turn. And here is the connection between identity, a group, a role, and permission to access a service.

This provides a useful degree of indirection: users are not granted rights but are only permitted by being a part of the role. The administration of user rights has been made easier since it now just needs the assignment of suitable responsibilities to the user/account. employee's Maybe most significantly, this strategy not only prescribes a way to define the responsibilities of data scientists (and other scientists in the company) but also simplifies permission management and helps to prevent misunderstanding that may lead to mistakes that cause security concerns [17]. RBAC is often referred to as IAM, or identity and access management along with identity management.

F. AI as a catalyst for cloud rethinking

The march to company AI on the cloud has begun. And it appears obvious that previous security methods could not maintain AI's data hunger. This has stopped the company's deployment of AI, requiring companies to transition to a contemporary identity-based security strategy.

New security methods based on identification are certainly more complicated than previous ones. And to manage and synchronize identities and responsibilities between the company and its cloud tenancy requires a new degree of rigor. Nevertheless, in sector after industry, the need for AI in the company is increasing [17,18]. And companies are now starting to reconsider their cloud safety policies. It would seem that identity-based security is not only a preliminary need but maybe a catalyst for altering the conventional cautious security posture of companies that enable AI adoption in the cloud to grow once again.

IV. FUTURE OF RESEARCH

The future in the U.S. Identity and Access Management (IAM) of AI is certain to become more and more part of our personal and corporate life in America as the technical and social environment continues to evolve quickly. The expectations are always high for excellent digital experiences. CIAM's advances enable businesses to fulfill these requirements by providing simpler, more secure consumer access to their websites and applications. Access needs for enterprises have drastically changed. Authentication procedures have meanwhile failed to keep pace, as shown by prevalent password-based restrictions. Every year, more than 60% of companies suffer a security violation, and about 40% of them occur because of a compromised user password [18]. Traditional, high-friction password procedures are often unsuccessful since they depend on end-users who always remember changing, complicated passwords. And when users confront robust authentication techniques, security procedures are typically more efficient in performing job duties.

AI-powered Adaptive Access Management offers an impressive option. Without human involvement, these systems can acquire and analyze user information to visualize and contextualize risk, discover danger trends, and adjust authentication procedures and access control dynamically. For example, businesses may establish rules that prohibit high-risk users from starting customer data apps without verifying their identity by high-safe MFA factors such as fingerprint or physical tokens. The cloud race drives demand for scalable security solutions "as a service" – and Access Management is no exception. Companies utilize SaaS-supplied Access Management to facilitate deployment and usage, provide strong, end-to-end security and offer a variety of operational advantages [18].

V. ECONOMIC BENEFITS

Management of identity is critical for the continued growth of the US Internet Economy. The US government and business organizations value trustworthy digital identities since the digital economy cannot work successfully without them. A collaborative study report produced by the Secure Identity Alliance (SIA) and the Boston Consulting Group (BCG) showed in 2014 that "moving digital" may provide saving annually to governments across the world [18]. The self-service, automation, tax collecting, and digital signature of citizens were only a few methods to save money by moving into the digital economy. The real benefit of the digital economy, however, goes beyond control and reduction of costs. Governments as providers of essential online services to entire populations can take the lead in promoting high value-added digital economic and social interactions: from expanding online commerce to strengthening democracy and personalized health services, to creating a whole new citizen-to-city economy, in which private individuals can provide services for each other through a trust

VI. CONCLUSION

This paper reviewed how identity management works for enterprise AI and cloud solutions. The findings from this paper show that digital identity has developed into an important component of enterprise AI on a cloud. They are no more basic and isolated individual information, but sophisticated websites which span the Internet, personal data, digital history, and the conclusions that algorithms make from it. Our digital identities are more and more integrated into our everyday lives. Verifiable digital identities provide value for companies, governments, and people alike. However, in this fast-changing environment, there is a lack of common principles, standards, and coordination across different stakeholder initiatives. The idea of identity has grown to include not just human users but also gadgets and apps, presenting a challenge for the people responsible for identity management. Hundreds or even thousands of identities may regularly use resources throughout a corporate network with their own unique set of circumstances. The introduction of AI and cloud solutions is always focused on everything, and a computer can identify subtleties that humans cannot. Complex network-wide interaction is becoming apparent, allowing IT professionals to execute better administrative operations and take more educated user authorization choices.

REFERENCES

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

[2] A. Farrokhi, F. Shirazi, N. Hajli and M. Tajvidi, "Using artificial intelligence to detect crisis related to events: Decision making in B2B by artificial intelligence", Industrial Marketing Management, vol. 91, pp. 257-273, 2020.

[3] M. Gartner, "Gartner predicts the future of identity and access management | IT World Canada Blog", IT World Canada - Information Technology news on products, services and issues for CIOs, IT managers and network admins, 2021. [Online]. Available: https://www.itworldcanada.com/blog/gartner-predicts-the-future-of-identity-and-access-management/443717. [Accessed: 20- Jul- 2021].

[4] U. Kerzel, "Enterprise AI Canvas Integrating Artificial Intelligence into Business", Applied Artificial Intelligence, vol. 35, no. 1, pp. 1-12, 2020.

[5] Z. Lei and L. Wang, "Construction of organisational system of enterprise knowledge management networking module based on artificial intelligence", Knowledge Management Research & Practice, pp. 1-13, 2020.

[6] D. McDougald, "Focus on Identity Management for Cloud Security | Accenture", WordPressBlog, 2021. [Online]. Available:https://www.accenture.com/usen/blogs/security/cloud-security-identity-management. [Accessed: 20- Jul- 2021]

[7] P. Mikalef and M. Gupta, "Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance", Information & Management, vol. 58, no. 3, p. 103434, 2021.

[8] D. Shackleford, "Get to know cloud-based identity governance capabilities", SearchCloudSecurity, 2021. [Online]. Available: https://searchcloudsecurity.techtarget.com/tip/Get-to-know-cloud-based-identity-governance-capabilities. [Accessed: 20- Jul- 2021]

[9] D. Strom, "What is IAM? Identity and access management explained", CSO Online, 2021. [Online]. Available: https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html. [Accessed: 20- Jul- 2021]

[10] I. Upadhyay, "Identity Access Management: Why Is It Important?", Jigsaw Academy, 2021. [Online]. Available: https://www.jigsawacademy.com/blogs/cloud-computing/identity-access-management/. [Accessed: 20- Jul- 2021]

[11] Cybersecurity Review, "4 Trends Shaping the Future of Identity and Access Management", Thecybersecurityreview.com, 2021. [Online]. Available: https://www.thecybersecurityreview.com/news/4-trends-shaping-the-future-of-identity-and-access-management-nwid-115.html. [Accessed: 20- Jul- 2021].

[12] D. Elliman, "The future of identity management", Thoughtworks.com, 2021. [Online]. Available: https://www.thoughtworks.com/insights/blog/future-identity-management. [Accessed: 20- Jul- 2021].

[13] J. Lovelock, "What The Future Of Identity Holds For The "New" Workplace", Facility Executive, 2021. [Online]. Available: https://facilityexecutive.com/2021/07/what-the-future-of-identity-holds-for-the-new-workplace/. [Accessed: 20- Jul- 2021].

[14] S. Neyman, "Four Trends Shaping the Future of Access Management", Cyberark.com, 2021. [Online]. Available: https://www.cyberark.com/resources/cyberark-identity/four-trends-shaping-the-future-of-access-management. [Accessed: 20- Jul- 2021]

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

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

[17] W. Ashford, "How to manage non-human identities", ComputerWeekly.com, 2021. [Online]. Available: https://www.computerweekly.com/opinion/How-to-manage-non-human-identities. [Accessed: 20- Jul- 2021].

[18] D. Gupta, "Council Post: Guard Digital Identity With Artificial Intelligence", Forbes, 2021. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2021/04/06/guard-digital-identity-with-artificial-intelligence/?sh=db12cfc6bca1. [Accessed: 20- Jul- 2021].

[19] I. Nikolova, "The Interaction Between Artificial Intelligence and Identity & Access Management - Patecco EN", Patecco EN, 2021. [Online]. Available: https://patecco.com/en/?p=1530. [Accessed: 20- Jul- 2021].