Intelligent authentication for identity and access management: a review paper

Ishaq Azhar Mohammed

Sr. Software Engineer & Department of Information Technology

London, UK

Abstract-*The main purpose of this paper is to explore how identity and access management systems provide important benefits in various enterprises. Identity and access management (IAM) systems usually consist of predefined tasks as an information security system. The authentication process is the most important function, as it is responsible for validating the identity of users for service providers that collaborate with another IAM [1]. This provides an analysis of how intelligent authentication work for IAM systems. The findings are assessed in light of the concept of intelligent authentication key factors, which is discussed below. Based on this assessment, it was not possible to study and execute an authentication that satisfied all of these main factors. To manage modern diverse and complex IT systems effectively, users must be assigned distinct identities and associated responsibilities to get access to each needed application, operating system, and databases platform. Users must remember numerous passwords, and IT must repeat an effort to provide and manage users on every platform [1]. This affects productivity and raises the danger of improper access to important data and other corporate resources for a user. There is a solution in the form of a unified and intelligent technique to identity and access management (IAM). Companies may condense every user's many identities into a few or, preferably, just one identity and establish a unified set of roles, and rules. This method greatly simplifies IAM administration, increases user and IT efficiency, and optimizes security and compliance. This paper will therefore discuss in detail how the intelligent IAM authentication method streamlines a variety of important activities, such as authentication via multifactor or password management.*

Keywords: *Identity and Access Management (IAM), Identity Management strategy, Access management, IAM enterprise*

I. INTRODUCTION

Historically, software programs within a company's information system have been built and put within the institution's perimeter. Hence, the company has a "safety zone" established by static techniques that are built and maintained by the IT department's personnel. In most instances, the 'trust area' encompasses the network infrastructure of organizations, application systems, which are maintained in-house as a data center. Alternatively, specialists inside the company administer or outsource the server farm to an alternative site but have control over how the security policies are built and implemented. Accessibility to the information resources of the company is protected in a "conventional" paradigm via a series of multidisciplinary mechanisms at the network level [2,3].

An authentication technique that is based on the automation of identities necessary to get access to the network with sufficient confidence is one of the most critical challenges in the field of information systems. An entity's identity is a set of well-defined characteristics that distinguishes it from other entities [3]. A company's information system interface is often installed and put within the company's limits. Therefore, the company has a "trust area" established by suggested strategies that are handled by the specialists. Digital identity is a series of characteristics that an entity owns and uses information technologies to define an identity (a person, company, application, or device). It is usually managed using Identity and Access Management (IAM), which ensures that the right people have access to the appropriate resources at the appropriate times and for the appropriate purposes [4]. This user authentication includes three tasks and activities which include identification, enrolment, and verification. The 1st and second 2nd subtasks pertain to the description and registering of digital user characteristics used for verification. Such parameters and configurations are often agreed upon by IAM and service providers. The final task is performed when a user tries to access a specific service platform through IAM [5]. This verification procedure is the key stage of any authentication system since it gives the user's identification and determines whether or not it is authenticated. Traditionally authentication relied on several variables, knowledge-based techniques, and possession-based procedures which had various problems. For instance, an authenticating password relied on the easy matching of the digital signature (password) in the claimed individual's knowledge and the secret phrase recorded in the system [5]. The outcome of this matching process was 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.

II. PROBLEM STATEMENT

The main problem that this paper will solve is to explore how intelligent authentication is significant for identity and access management and its operations. The primary issue that this article resolves is how intelligent authentication is important to the management of identity and access and its activities. The complexity and variety of the IAM features have always been considered a necessary evil. Even so, innovations (apps, computer systems, and networks) need different identities, functions, processes, and permissions in every organization. Such limitations imply that the IAM needs two things in most corporations:

unity and intelligence [5,6]. This is based on the consideration of the advantages of unification of identities, roles, processes, and confidentiality agreements to offer a single all-powerful smart IAM strategy that impacts every platform, user, environment, and need (security-related, operational, and compliance-driven). If this were feasible, IAM would instantly transform from a difficult, costly, and frustrating endeavour into an organized, attainable, and personally optimized strategy that propels a company ahead instead of holding it back. Intelligent Authentication (IA) helps avoid untrusted sources of fraudulent account sign-in. Intelligent authentication is a complement to or a replacement for conventional hardware and mobile identities in identity and access management [6]. IA offers the end-users with layered safety with minimum user experience interruption. IA security layer utilizes "risk-based" authentication to evaluate many profile information along with the username and password as well as login credentials common for every login user. This procedure assists corporate web developers and information technology experts in integrating intelligent authentication into their online applications. In this case, IA allows users to sign in securelyc[6]. Clients must set up the Smart Authentication policy in the Manager tool before using IA encryption for the end-users.

III. LITERATURE REVIEW

A. Traditional IAM Strategies

It has long been accepted that IAM components are complicated and diverse. A company relies on technology, where such technologies need distinct identities and duties, processes, and authorization [6]. The IT staff must devote resources to each to guarantee these technologies deliver on their expectations. Then there's the ever-changing realm of security and compliance, which demands greater degrees of management and visibility. It is a continuous fight to do things at the cheapest feasible price, without jeopardizing security and compliance. And besides, IAM is a tool for running your company, not the primary reason why your organization exists. Two main methods have historically motivated attempts to manage IAM's complexities:

Using point solutions: Companies attempt to meet particular requirements of individual systems through point solutions, such as implementing and synchronizing the self-service password reset option in one platform [6].

The use of an IAM Framework: The option is to create a comprehensive framework that can be tailored to the particular environments, needs, and objectives of an organization. Examples are IBM products like Tivoli Identity Manager, Oracle (especially newly acquired Sun technologies), Novell solutions, IT associates, and Microsoft's Forefront Identity Manager, which is the latest entrant into the industry [6,7].

These methods may offer value and get companies nearer to their goals, but neither approaches to address the fundamental source of all the problem, which is too complicated. Identity, roles, rules, and policies are still handled individually, inconsistently (in the context of application services), or costly with custom programmed logic (in the case of an IAM

framework). In addition, compliance and safety are frequently reactively rather than proactively handled [7].

Handling particular requirements using point solutions simplify some processes and makes the target system more secure and compliant, but does nothing for the other components. The intricacy persists, and new point solutions have to be developed to meet specific requirements in many other systems, leading in an, even more, disassociated context with more instruments and IT workload [8].

B. A Cohesive and Intelligent Approach to Identity and Access Management

When all elements of an IAM strategic approach were unified—that is, if each user had a single identity throughout all platforms, a fixed set of functions that could be automatically added wherever they were necessary, a single set of processes independent of the body systems, as well as a single set of authorizations powered by business requirements instead of technological advances identity and access would've been easy, cost-effective, and secure [8]. Is it possible for the company to get there? Everything developed over the years and restarts with a new beginning as well as a single IAM authorization provider and would be almost difficult to completely abandon. Nobody is in a capacity to completely restructure their infrastructure around Microsoft technology, Oracle technologies, or Linux solutions [8]. Indeed, most of the usefulness of technology is derived from the variety of available choices and the ability to choose the most appropriate technology for a particular requirement. Fortunately, integrating identity and access management does not have to be a zero-sum game. It is feasible to significantly decrease the number of business IDs. Consolidating disparate and Adhoc roles, processes, and attestations into a more uniform and consistent set is feasible [9]. In other words, you may retain the appropriate level of technological variety while streamlining the major aspects of IAM—identities, functions, procedures, rules, processes, and attestations.

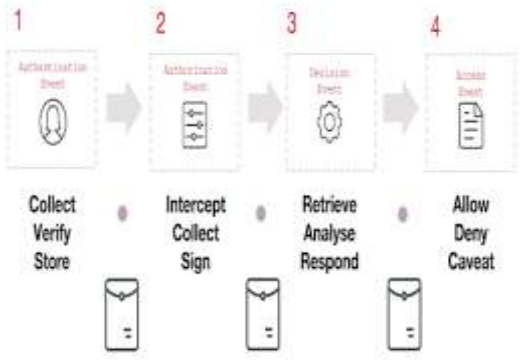

Fig i: Intelligent authentication process

The Critical Features of a Unified and Intelligent Approach to Identity and Access Management

Key elements of a new unified and intelligent solution to IAM include the following:

• Integrating every identity into a single, previously existing identity whenever feasible [9].

• Developing a unified set of priorities, policies, activities, and authentication for that single identity, which often manages a much greater part of the business.

• Addressing critical issues with point solutions that are completely compatible with the unified identity domain. Examples include using AD-based enterprise single sign-on in platforms that must be integrated with AD, including platform-specific privileged managed services that rely on AD roles and identities for tailored assignment of privileges, among other things [9].

• Consolidating everything (unified and non-unified systems) in identity intelligence that understands and transforms all current roles, regulations, processes, and attestations into a given model that achieves authentication using business goals and technical capabilities—as the driving force [10].

C. Utilizing an Identity and Access Management Framework

IAM frameworks are frequently seen as the sole method to implement IAM. Nevertheless, they were typically custom-made and made extremely costly for lengthy development and implementation cycles. The overwhelming majority of businesses are either unable to finance a framework or opt-out of undertaking a project of this magnitude. Furthermore, IAM frameworks, like point solutions, do nothing to address the problem and complexities of IAM [11]. In this case, the framework will always need all 10 identities, plus the 11th identity in a meta-directory that governs all the others. When five distinct copies of the registered user exist across the necessary systems, then the IAM framework may need custom-built business logic to deal with the variations and idiosyncrasies from each. Ultimately, all processes and attestations must be customized inside the framework, sometimes copying software applications or needing new components to replace ad-hoc ones [11].

D. Multifactor Authentication

To comply with a variety of government and industry requirements as well as security practice guidelines, identity verification must be strengthened beyond the degree of protection provided by a basic username and password login. This robust access control method combines two to multiple elements, including smart cards, one-time passwords (OTPs), or even biometrics, to check the identification of a person before giving access to them. Every option adds "what users know," "things users possess" (smart card or OTP tokens), and/or "what they are" to its user account [12]. Deploying multi-factor authentication services may be costly since conventional solutions need extra specialized infrastructures. Additionally, the solutions may be challenging to maintain, especially when multifactor authentication is required across various, non-integrated systems. It is very unusual for users through secure communications information technology settings to have several smart cards or OTP tokens hovering on their key chains, one per platform that needs to be accessible.

Numerous multifactor authentication providers have successfully persuaded their clients that the unique layout and short lifespan of multifactor authentication systems are essential [12]. Nevertheless, technological and cognitive advances have shown that multifactor authentication will not have to depend on proprietary services and also that non-expiring features are possible. Every multifactor authentication in new OTP systems is based on Active Directory, not on a separate, proprietary directory, and adheres to regulatory requirements, allowing businesses to select configurations from a variety of manufacturers [12].

Fig ii: Multifactor authentication

I. A Unified and Intelligent Approach to Multifactor Authentication

IAM unification is the key to multifactor authentication advances. For instance, Unix, Linux, Mac, and Java platforms that have integrated Active Directory may be protected using the same multifactor authentication method as AD, removing the requirement for a handful of tokens or a stack of smart cards. For example, for any Unix, Linux, Mac, or Java platform which is established as a component of the AD – trust realms – Quest Defender offers one-time password (OTP) verification using Quest Servers [13]. Additionally, Authentication Solutions expands its reach to Unix and Linux platforms for companies that already have a Windows smart card setup. Additionally, Quest Enterprise Single Sign-on may be configured to start SSO using any multifactor authentication method (smart cards, OTP,

or biometrics). Although the identity intelligence framework has no significant impact on multifactor authentication, it can add another layer of command and accessibility to it depending on the unified identifications, roles, guidelines, policies, business processes, and attestations that could necessitate multifactor authentication for direct connections or are required to provision and maintain the multifactor authentication platform [14].

E. Password Management

When users of a given platform have numerous identities, they often have multiple passwords, which is another security risk. It creates the following challenges:

•Inconsistent password practices - Because various systems need unique passwords, it is quite challenging (and in certain cases impracticable) to create a single, safe

strategy for all passwords [14,15]. Many platforms may not handle the same level of password complexity as others, and IT professionals may have more pressing priorities than abolishing and rebuilding password rules to align with the rest of the business.

•Password resets are costly-This is because the more the number of passwords that users must memorize, the greater the likelihood that they will lose them, leading to a loss of productivity for workers and greater IT workload. In reality, an IT specialist is frequently needed to change passwords that seldom form part of the primary work of the employee [15].

•Security and compliance problems - Whenever users are required to memorize a large number of passwords and the criteria for selecting passwords to change across systems, they take precautions such as jotting down personal passwords [15].

I. Password Management: A Unified and Intelligent Approach

Allowing users to change their numerous passwords is insufficient—the aim must be to minimize the number of passwords the user is required to remember and what IT staff must manage. A unified approach to IAM does just that: by unifying identities across Unix, Linux, Mac, Java, and a large number of standards-based tools, which eliminates the need for these platforms to use passwords. Consequently, these passwords must not be changed, and users must not break security and compliance regulations by writing them down [16]. Additionally, a single strong password rule may be established across the full spectrum of AD-integrated applications, and multifactor authentication could be utilized to improve security even further.

Fig iii: Password management authentication

IV. FUTURE IN THE U.S

Authentication is changing, and the future is apparent. More complicated passwords or passcodes, as well as improved multi-factor authentication, are not in the cards for the future of authentication. The United States is transitioning away from static, password-based authentication and toward intelligent, continuous authentication and authorization. The fact that a large majority of Americans place a higher value on the ease that IT companies offer to banks over privacy makes it more essential than ever for financial institutions to do their bit to safeguard customers from identity fraud and money laundering [16]. Nonetheless, before contemplating the use of an AI-driven authentication mechanism, financial institutions must evaluate their existing infrastructure capabilities, as well as their ability to offer biometric and behavioral capabilities. There is expected to be a significant increase in evolution in the background, with such changes being completely undetectable to the user. These advancements are expected to be focused on constant monitoring and seamless engagement: detecting risk- and behavior-based authentication [17]. A user's permission to access data services is determined by current authentication systems, which check whether or not the user has the right to do so. Both username and password are the most often used authentication elements; in simple words, a single-factor authentication technique is used. To utilize multifactor authentication (MFA), a user must provide more than one authentication source, such as a password and evidence of identification, such as by inputting a PIN received through text message. Using a second authentication method will take more effort from the users, but it will also offer extra safeguards for the information that has been restricted. Despite its possible drawbacks, multifactor authentication will be discussed in the future when it comes to access control strategies. Multifactor authorization, on the other hand, is not going anywhere. As more and more Internet of Things devices become a part of everyday life, trustworthy web pages will require more than 3 information sources [18].

V. ECONOMIC BENEFITS

A smart authentication system for identity and access management may very well be the future of assisting financial institutions in the United States to enhance customer satisfaction by streamlining access and security. Several technologies, including machine learning, cloud computing, and analytics, will be critical in decreasing human error in a wide range of sectors, including banking [18]. In the United States, the use of artificial intelligence to fight hackers and make mobile applications a safer location to conduct transactions and establish bank accounts has the potential to completely transform the banking sector. There are lots of robust authentication solutions available now that will both safeguard consumers and prevent U.S. companies from being subjected to large penalties and expensive security events in the interim. Decentralized solutions will allow users to regain control over their identities while still offering one-touch access to resources [19]. To put it another way, everyone on the planet will be the owner and controller of their own legal identity.

VI. CONCLUSION

This research paper explored how intelligent authentication may be used in identity and access management, with a particular emphasis on multifactor authentication and password management. The study findings showed that identity and access management become complex, especially if a diversified IT infrastructure requires numerous identities for each user. Such complexity often leads to fragmented methods to role administration, user authentication, and provisioning, as well as haphazard efforts to multifactor authentication as well as privileged account management that are based on "doing the best we can with what we have." It is important to limit complexity, simplify processes, and add a layer of management that is determined by organizational goals rather than by IT or technological capabilities via the use of a unified and intelligent approach to information asset management. Intelligent authentication, in particular, minimizes the number of identities that may be linked with a single person by a factor of two. This simplifies critical identity management activities like password resets and audits, while also increasing security via the use of multifactor authentication. It also removes the keys to the kingdom issue by distributing administrative access in granular increments and by maintaining an audit record of administrator privileges and actions, among other things. It also consolidates user passwords and provides self-service password changes, which improves security while simultaneously increasing efficiency for the organization. In general, intelligent authentication enhances the current IAM framework to reduce complexity, which reduces costs, improves control, and accelerates time-to-value while also lowering costs and increasing control.

.

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] C. Xiong, Intelligent robotics and applications: first international conference, ICIRA 2008, Wuhan, China, October 15-17, 2008: proceedings. Pt. 2. Berlin: Springer, 2008.

[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] 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.

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

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

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

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

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

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

[15] H. Sasaki, Intelligent and knowledge-based computing for business and organizational advancements. Hershey, PA: Information Science Reference, 2012.

[16] J. Sołdek and L. Drobiazgiewicz, Artificial Intelligence and Security in Computing Systems. Boston: Springer US, 2003.

[17] R. Sharman, S. Smith and M. Gupta, *preview this item Get a Copy Find a copy in the library Digital identity and access management: technologies and frameworks*. Hershey, PA: Information Science Reference, 2012.

[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.