JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A literature review on the tools for Identity Access Management using AI

Shabana Mulla

Sr. Faculty member of Department of Information Technology

Pune, India

Abstract- *The purpose of this research is to explore how artificial intelligence may benefit in the context of identity and access management in a cloud computing environment. With the increasing use of cloud technologies, security, compliance, and operations, teams must contend with a host of new issues. Despite the operational benefits of cloud platforms like "AWS, Microsoft Azure, and Google Cloud Platform (GCP)", they also present additional problems for an organization's ability to secure data in the cloud and meet ever-increasing regulatory requirements. The identity and access management system (IAM) is a prime requisite in cybersecurity in any organization. In addition to mitigating data breaches, it also helps to manage the risks associated with working remotely (especially after covid times) and bringing your device – BYOD – into the workplace. Internal data synchronization, customer contact preference management, and fulfilling privacy compliance standards are just a few of the important tasks that IAM is continuously developing to handle in the modern world [1]. It is important to develop a well thought and well-developed IAM strategy. Determining who should have access to what information is a tough decision for many companies, and this difficulty makes their information systems insecure. Forrester's study found that 83 percent of companies do not have a mature strategy for identity and access management (IAM). When compared to companies that have implemented their IAM strategy, these companies are twice as likely to have difficulties because of a security breach [1]. We have found a clear positive correlation between better IAM methods and decreased security risk, enhanced productivity, greater privileged activity control, and reduced financial losses, according to the study. A comprehensive and smart solution to Identity and Access Management (IAM) is an integration of artificial intelligence against the cyber security risk in cloud computing. Companies have been able to condense the many identities of each user into a couple or, preferably, one identity and establish a single set of responsibilities, rules, processes, and proof of that identity. This method substantially automates IAM utilizing artificial intelligence, which enhances user and IT efficiency and optimizes safety and compliance. This paper demonstrates how the intelligent IAM interacts with artificial intelligence to streamline many important tasks such as identity management in the cloud computing environment.*

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

I. INTRODUCTION

In the most critical challenge of data, security is making a trusty authentication mechanism supported by digital identity. A digital identity is the assortment of information concerning a person, organization, or device that exists online. Identity and access management (IAM) is the discipline that permits the correct people to access the correct resources at the correct times for the correct reasons. Whenever a user tries to access a service supplier system through IAM, the verification method is a very important stage in any quiet authentication system since it establishes the identity of the user and determines whether or not he has been licensed. conventional authentication depends on a spread of variables, techniques suffer from a spread of issues. using the instance of a password authentication technique, the disclosed users' secret phrase (password), yet because the secret phrase that has been stored within the system, are merely compared [1]. the result of this matching method is employed to ascertain the identity of the claimed user in question. There are several problems with this methodology, as well as the chance of the key phrase being purloined or forged.

This paper can examine how AI is getting used in identity and access management, yet because of the challenges that are encountered.

II. PROBLEM STATEMENT

The problem that this research will seek to resolve is to explore how artificial intelligence plays a prominent role in improving the security of identity access management. The indicators of malignant behavior include unauthorized logins, many time attempts of wrong login and password in a short period, requests from malicious sites, using unauthorized technologies, and connection using an illegitimate network instead of the organization-protected network.

Traditional IAM solutions that focus only on authenticating users during login might not detect a user a threat actor stole and then used whose credentials are overseas. But a modern AI IAM platform detects anomalous behavior, even after a user has logged in, and can trigger an alert to block access. AI can find even the smallest anomalies that can indicate it has compromised credentials. AI analyzes data to understand the relationships between users, data, and things. This can be used to create granular policies without impacting user experience.

Identity and access management (IAM) is becoming more powerful with artificial intelligence (AI), which allows

organizations to provide a detailed and adaptable response to authentication and access control.

LITERATURE REVIEW

A. What is Identity and access management (IAM)

Identity and Access Management (IAM) is an inclusive term that refers to the framework of rules, regulations, and technology used to guarantee that only authorized individuals within an organization have proper network access [5]. Access control to a company's assets is provided through identity management systems, which also monitor user behavior while we log them into those resources. The IAM enables the management of user authorizations depending on organizational roles [5]. It achieved this by providing a method of safeguarding corporate resources and data via rules and regulations that require login passwords, well-defined user rights, and access control, among other features. IAM is a process of integrating rules and regulations for effective security systems [6]. Applications for identity and security management are also essential concerns. Access requests to secure business documents are verified by IAM, and users are either granted or denied access based on their request. The major task of IAM is managing user identity, IAM systems can be solely responsible to create, modifying, and deleting users and creating new identities for users who need a specific type of access to particular organization tools. Provisioning and de-provisioning users, defining which tools and access levels (editor, viewer, administrator) to grant a user is called provisioning. IAM tools allow IT departments to authorize users by role, department, or another grouping in consultation with the organizing authority. Since it is time taking activity to specify each individual's access to every resource, identity management systems enable provisioning through policies defined based on role-based access control (RBAC). Users are assigned one or more roles, usually based on the function of the job, and the RBAC IAM system automatically grants them access.IAM can also use to avoid security and quickly remove ex-employees' access. IAM systems authenticate a user by confirming that they are whom they say they are. IAM Access management ensures a user is granted a definite level and type of access to a tool that they're designated to. Users can also be divided into groups or roles so a large portion of users can be granted the same privileges. IAM tools help in generating reports on the basis of user activity on the platform (like login time, systems access, and type of authentication) to ensure compliance and assess security risks. The management of user life cycles, different application accesses, and single logons are all examples of IAM standards and applications [6,7].

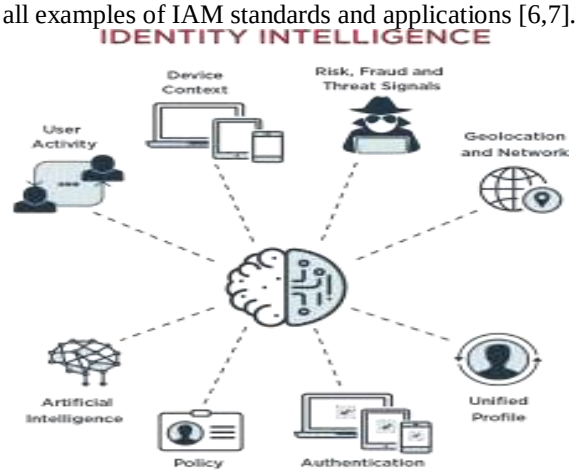

Fig i: IAM platform utilizing AI

Authentication and access control are required for data security. Correctly implemented IAM systems may improve employees' performance by enabling them to access data through different application places and devices. It also makes it possible to communicate and collaborate more effectively with other companies, suppliers, and commercial partners.

B. Artificial Intelligence in action with AI

There are many benefits to using IAM, including improved business value and security, better work efficiency, and a decrease in the burden of IT personnel.

IAM helps employees as well as Contracting companies and business partners, distant and mobile users, as well as consumers, to access company resources securely. With digitization, they allocate identities to the Internet of Things (IoT) devices, robots, and bits of code, such as APIs or microservices, as well as to people and organizations [10]. Multi-cloud hybrid IT systems and software as service (SaaS) solutions add to the complexity of the identity and access management (IAM) landscape. When implemented properly, information asset management (IAM) helps to guarantee corporate efficiency and the smooth operation of digital systems.

one very important area where artificial intelligence (AI) is used in cloud computing IAM is for user and entity behavior analytics (UEBA), which is used to detect malicious activities of the users. With the help of machine learning and deep learning algorithms, it makes statistical analyses to know when there is a deviation from regular patterns, showing which of these deviations could result in a potential, real threat. UEBA can also scrutinize the data from user reports and logs, as well as analyze user files, flow, and packet information to identify likely threats. Microsoft offers Azure Active Directory (AD) Identity Protection, which implements machine learning to detect malicious user behavior. IT experts need not necessarily know how to implement machine learning techniques to benefit from Identity protection, but still they can send Microsoft any false positives that the system detects to improve the algorithms. IBM's cloud identity and access management solution provide software that offers AI-powered, risk-based authentication, and more advanced features. Deploy as multi-tenant SaaS in an IBM Cloud center, or single tenant dedicated to certain residency requirements.

Other products, such as Oracle Adaptive Access Manager and RSA Adaptive Authentication, enable IT, experts, to modify the machine learning models themselves, a very important potential power that typically appeals to larger organizations that already experience specific cyberattacks. Experienced IT experts can tweak machine learning models to reduce false positives and gain a more granular level of control.

Ever since AI has introduced it has proved to be more capable than humans in noticing and facilitating all domains which need our specific attention. A recent report from Forrester has assured that Artificial Intelligence embedded software will be a very common occurrence by 2023. Even now, these AI systems can collect the underlying information of where there could be a breach in security, analyze those points, and proactively protect the user's identity.

Adaptive multifactor authentication is all about collecting accurate information. The information is collected by the AI and processed as per this, a risk score is calculated. This risk score decides the method of authentication for the users.

Low risk: only accepting passwords is enough for the login process.

Medium Risk: it is to implement MFA to ensure identity.

High Risk: Complex authentication steps are taken, and the system notifies the user through the registered email address and phone number about the malicious activity.

The elements that are considered when calculating the risk score are

Time of Login: if login attempts within a few minutes of the

initial login process, then there is a possibility for the data to be stolen.

Location: If a user typically makes an attempt to log in from two different locations, then it will make Artificial Intelligence (AI) systems suspicious.

IP Address: If the user tries to log in from the same IP Address. But making changes in the address initiates Artificial Intelligence reconfirming the user's identity.

Identity and access management tools with AI can also use analytics to more precisely determine when they actually need multifactor authentication and cut down on its usage to improve the user experience. For example, an IAM system can evaluate attributes such as user login location, fingerprint on the device, and IP address and automatically grant access if the combination is low risk. An organization that uses this functionality practically reduces its employees' usage of MFA and passwords by ninety percent. Mobility simultaneously complicates and simplifies multifactor authentication. either, it can use mobile devices for verification purposes in multifactor authentication, either by sending SMS or by using the device itself as a token, or in case of low-risk based login, no password technologies can help to avoid multiple authentications altogether. The Productivity type of mobile app permits managers to track the activity of their staff on mobile devices, and it doesn't require the manager to enter a password when accessing the app. If Auth0 recognizes that the user is on an employer-owned phone, it sends them an email with a link that will complete the login process and does not compel them to log in again in the future.

The Bernard Group, a communications provider in Chanhassen, Minn., uses ManageEngine's AD Manager Plus to handle MFA for end users' access to email and cloud-based applications.

Authentication monitored by Artificial Intelligence (AI) has a much larger scope. Instead of just sticking to processing login attempts, they could constantly monitor a user's behavior to detect any breaches in security. It could also come to a point where the AI decides on the number of factors that must be implemented to ensure the security of a profile!

Based on the outcomes provided by the AI systems, it can implement machine learning algorithms to further refine the authentication process.

One of the most famous and very user-friendly methods of authentication is biometric verification. Bio matric technology can be divided into two physical biometric technology and behavioral biometric technology There are several methods by which physical biometrics can be implemented:

AI Deep learning, especially convolutional neural network (CNN) has made tremendous success in the field of computer vision and pattern recognition as it does not require handcrafted feature extraction. Deep learning automatically learns features and structures under enough training data. These advantages of CNNs make them suitable for various tasks in automatic fingerprint recognition/identification systems:

The Iris recognition, every single person in the world has a unique iris pattern, and they process this with image processing techniques, and they use an AI decision tree algorithm for the classification.[19]

Voice recognition, when we give any vocal input, takes in the analog data, and converts it into digital data with the help of AI neural networks and machine learning automatic authentication process becomes beneficial.

In face recognition, the image of a face is captured, and details like the alignment, size, and shape of the face are analyzed and processed with deep learning techniques which helps an organization achieve a high level of automatic authorization.

Behavioral dynamics, another authentication technique that is implemented with machine learning, is by verifying the behavioral dynamics. Every individual human being possesses an ingrained behavior that machine learning algorithms could evaluate. Some of the user behaviors which could be studied are Keystroke dynamics: this analyzes the rhythm with which the user types the password on their keyboard.

Mouse dynamics, consider how the user interacts with the mouse or the touchpad.

Hardware interaction analyses deal with how a specific type of user handles their devices and their positional parameters.

such kind of data can be collected, and once the system is familiar with its user, it can detect identity changes with the change in these behavioral patterns.

Octa Risk-based Authentication, a feature of Adaptive MFA, uses machine learning to deliver automated detection and response to identity-based attacks. Okta transforms data inputs and variables, such as device, location, IP address, and biometrics, into contextual behavior profiles, which are quantifiable, actionable authentication and authorization. decision

AI-based authentication systems and predictive analytics using machine learning, deep learning, and Neural networks are making our life much easier. Soon, these techniques will go beyond the entry-level sign-in methods and encompass other areas where the security of the user data is essential.

The COVID-19 pandemic has upended how organizations orchestrate work. The inflated number of employees working from home using conferencing and collaboration services are stressing back-end support services and expanding traffic on networks that connect users to these services. Only providers with robust and abundant architecture that deliver uncompromising and secure customer experience shall be able to superintend the inflated load.

Remote work and technology are feasible and don't reduce productivity, some employees may never really return to physical workplaces. According to a recent study of finance executives conducted by the research company Gartner, seventy-four percent of respondents wish to perpetually devolve certain workers to remote work [11] The IT and security workforce would need to indistinctly describe their information protection rules associated with remote work that were either put in place or at the very minimum reviewed at the kickoff of the migration to a virtual force for those workers Virtual workforce can continue functioning from home [11]. In any case, businesses should contemplate the way to increase worker flexibility whereas still providing them with the mandatory technology and resources to continue operating effectively and safely throughout times of transition.

D. Artificial intelligence based on risk-based authentication

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

user with high-risk logins, IT administrators may ask users to provide an extra authentication factor, such as a Face ID or fingerprint scanning, or they can completely deny access to their online platform.

For low-risk logins, when users behave predictably, administrators may just ask the submission of an OTP number received through the authorized phone number or enable the user to skip MFA altogether.

It is an effective option for both users and organizations. When the context of a user's login changes extensively, MFA or other authentication factors must be used to prevent phishing and ransomware attacks.

Mobility simultaneously complicates and simplifies multifactor authentication. Mobile devices are used as an authorization and

authentication platform in multifactor authentication, either through SMS or by using the device itself as a token. Or password. fewer technologies can help IT avoid multiple authentications altogether.

The Produactivity mobile app will help superiors track the activity of their employees on mobile devices, and it doesn't require them to enter a password when accessing the app. If Auth0 recognizes that the user is on an employer-owned phone, it prompts them to receive an email with a link that will complete the login process for them, and they will not have to log in again in the future.

ForgeRock Identity Management fully automates the entire identity lifecycle management process.ForgeRock software development kits help you build secure digital experiences faster on the ForgeRock platform. By leveraging the SDKs one can bring apps to market faster and reduce costs and risk. The software enables easy integration of authentication, registration, and self-service journeys, allowing mobile and web apps to benefit from Intelligent Access.

Popular blockchain metaverse cryptos include Axie Infinity (AXS), Decentraland (MANA), The Sandbox (SAND), and Tamadoge (TAMA) use a combination of blockchain and artificial intelligence to enable trusted digital analysis and decision-making on huge amounts of data, it can be used to create secure data sharing and make artificial intelligence explainable, as well as regulating trust between devices that cannot trust each other.

E. Challenges and risks of implementing AI with IAM

Even though IAM is present at each level of an organization's information security design, it doesn't cover all the bases. One downside is the evolution of users' "birthright access" rules [13,14]. These are the access privileges permitted to the latest users throughout their initial day of employment at a business. once it involves granting access to new staff, contractors, and partners, the alternatives are several and bit a spread of various departments. This degree of automation becomes vital once considering machine-controlled onboarding and compliance management of users, user self-service, and in-progress compliance verification, consistent. Another downside is that, though zero-trust networks are quite standard right away, the challenge is having the ability to perpetually monitor these trust connections once new applications are introduced to a corporation's IT system design. we tend to monitor what people do once work and examine the baselines of behavior. There are several false positive eventualities, like if a user breaks their finger, which will destabilize these trust connections. Following that, the affiliation between identity and access management (IAM) and single sign-on (SSO) should be properly managed [15,16]. the mixing of identity and access management with customer-centric identity and access management has started, as shown by Okta's purchase of Auth0 [16]. as a result security consultants can still treat these initiatives one by one, it'll force IAM to play catch-up all the time.

Finally, IT directors should embrace identity management within the development of all new apps from the start. To with success pilot any IAM and identity governance initiatives by rigorously selecting a target app that will be used as a model and enlarged to further applications throughout the business.

How Artificial Intelligence Addresses IAM Challenges

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

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

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

As microservices and serverless design — a model during which a cloud supplier dynamically distributes resources — adoption grows, thus can the adoption of cloud-based identity and access management tools that are attractive to developers. Organizations will certify users of serverless applications on Amazon Cognito, for example, a federated identity management platform that allows developers to specialize in writing code rather than managing authentication

Finally, IT administrators should embody identity management within the development of all new apps from the start. To with success pilot any IAM and identity governance initiatives by rigorously selecting a target app that may be used as an example and later dilated to further applications throughout the business

II ECONOMIC ADVANTAGES

The rise in employment opportunities for the American market is at the heart of the economic advantages of adding artificial intelligence to IAM. The United States will be necessary to retain millions of individuals in the United States for them to survive in the workforce. Millions of employees will need help in adapting to the changes brought about by artificial intelligence, robots, and associated technologies. In the field of identity and access management, advancements in automation

and Artificial Intelligence (AI) have the potential to bring about levels of prosperity that humans have never seen. The economic advantages of IAM in the U.S also relate to the development of the Blockchain sector. Since something may individually verify identities in an unchangeable and secure ledger, blockchain technology may be able to address a variety of digital identity issues. Cryptocurrency systems rely on identity verification through public key cryptography-based digital signatures [18]. The sole verification done with this technique is to ensure that it verified the transaction with the proper private key. We deduce that the owner is the individual who has access to the keys. The identity of the owner is irrelevant. Biometrics enhances the capacity to verify a client's identification with a high degree of confidence, enabling automated onboarding and remote access to public services. A variety of biometric technologies are becoming cheaper.

III. CONCLUSION

This analysis evaluated how artificial intelligence (AI) is getting used in identity and access management, also because of the difficulties that are encountered and also in the scope of the industry's future. According to the results of this study, continuous authentication ensures that the context of a user is unendingly assessed at each contact. AI will analyze micro-interactions while considering time, location, and even user quality, and estimate the degree of attainable danger at every step in the manner. Any future development ought to incorporate cloud-based integration because the business shifts additional and additional to the cloud. I handle the event of IoT identity and access management via the mixing of contemporary strategies. Identity and access management is, therefore, a key element of any business data security as a result of it acts as a barrier between users and sensitive company assets. Identity and access management tools should further become developer friendly as vendors unharness modularized platforms. the method of drawing up one identity module to a different one, as an example, needs additional integration work by developers -- particularly if those 2 modules are from totally different vendors, attributable to that, vendors should provide integration capabilities exploiting the foremost fashionable development languages.

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[19] https://mobidev.biz/blog/ai-biometrics-technology-authentication-verification-security

[20] https://www.techtarget.com/searchmobilecomputing/news/252441320/Identity-and-access-management-tools-add-AI-microservices

[21] https://sennovate.com/how-artificial-intelligence-and-machine-learning-helps-in-mfa/