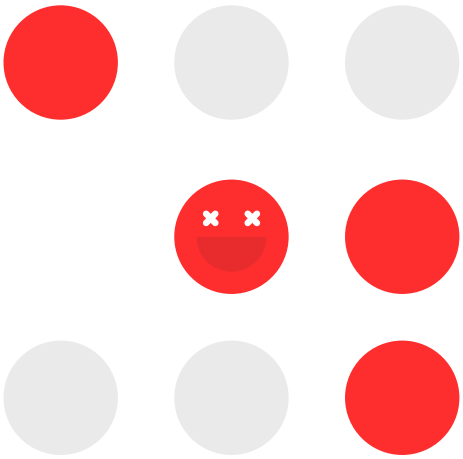
ManageEngine
AD360

FUTURE TRENDS IN

IDENTITY AND ACCESS MANAGEMENT

TABLE OF CONTENTS

Executive summary



Identity and access management (IAM) is an indispensable component in managing the privacy and security of an organization, and the acceleration towards digitization and the increasing demand for protection from identity theft, fraud, and cyberattacks emphasizes the need for competent IAM solutions and systems. As the number and complexity of cyberattacks continue to increase exponentially, it's critical for enterprises to secure their resources and follow proper IAM and cybersecurity practices.

The onslaught of the COVID-19 pandemic has resulted in an alarmingly high number of security breaches and cyberattacks, leading to what many called a cyber pandemic. As organizations all over the world are gradually adapting to remote working and hybrid working models, organizational assets now have to exist outside traditional security perimeters. Cloud adoption has also gained momentum, stressing the need for competent and robust IAM solutions to tackle these issues. Passwords are likely to be considered redundant, and organizations should instead focus on current and evolving technologies such as decentralized identities, Zero Trust, identity proofing, privileged access management, and cloud adoption. This report sheds light on the future trends in identity and access management based on recent predictions by industry experts.

Introduction

What is identity and access management?

Identity and access management, commonly abbreviated to IAM, refers to the tools, technologies, and processes used to manage the digital identities of users and their access to various resources within an organization. In other words, IAM is a way to determine who a user is and which resources they are allowed to access. An IAM system equips administrators with the tools and technologies required to create user identities, track activities, and manage the access privileges for each identity.

Identity vs. access management

IAM is composed of two processes: identity management and access management. Identity management encompasses the tools, technology, and processes used to manage digital identities throughout their life cycle. This includes functions such as creating, onboarding, maintaining, monitoring, and deleting the identities. These identities and their attributes are stored in a central database. The process of authentication is also included in identity management.

Identification

Identification occurs when a user claims an identity and it's the first step in access control. This identity comprises a set of specific properties, which can be digitally measured and recorded.

For example, a user can prove their identity by using their username and password to verify their email account. This verification process can be carried out by multiple authentication factors, which are explained below.

Authentication

In the authentication process, the identity of a user is verified using proper credentials called authentication factors. In the email account example provided earlier, the password is said to be the authentication factor as the user confirms their identity by providing the correct password for their account.

Authentication factors are generally based on the following criteria:

Something the user

- knows, such as a username or password.
- has, such as a key card or USB device.
- is, such as fingerprints or other biometrics.

Authorization

Authorization is the process by which the user is granted access or permission based on their verified identity. For instance, the user is granted the appropriate access privileges to their email account after being authenticated with the help of their username and password. This is the final step in access control. Based on their requirements and level of authority, each user is provided with specific access privileges.

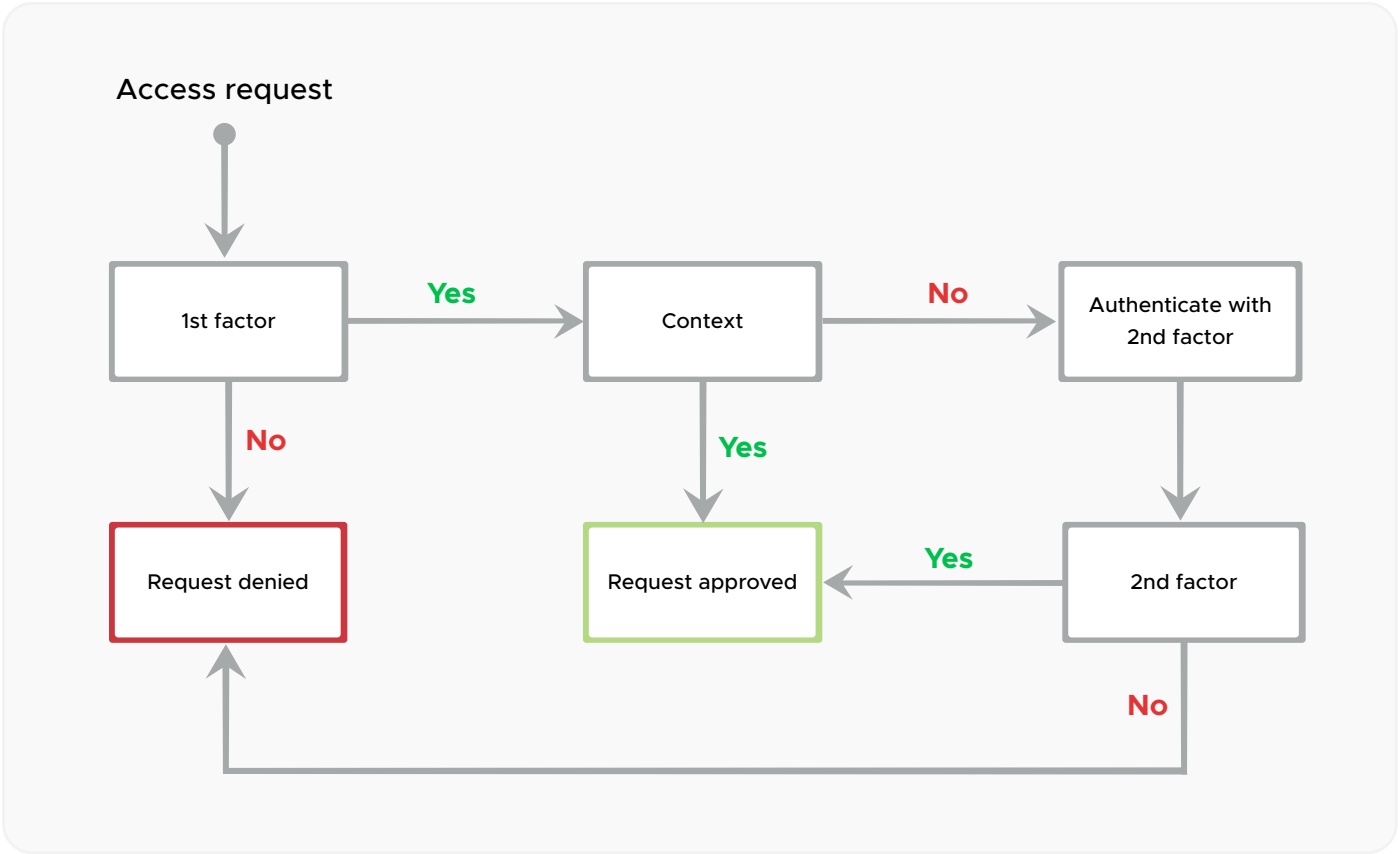
Access management refers to the processes and technology used to control the decisions which allow or restrict a user to access specific resources. This includes functions such as managing access requests from users and controlling access to resources. This is done by means of authorization, where the identity attributes are evaluated and decisions are made based on policies.

IAM tools and systems

Some of the different tools and systems that are deployed for identity and access management are as follows:

Multi-factor authentication

Multi-factor authentication (MFA) uses more than one authentication factor to grant access to the user. This is generally employed by combining multiple authentication factors—something the user knows, something the user has, and something the user is. For example, in a two-factor authentication (2FA) process, the user may have to provide a password and biometric information (such as a fingerprint) to gain access. Another example may be a one-time password or code sent to their device. Increasing the number of credentials or authentication factors required to gain access to the network provides an additional layer of security and reduces the occurrence of credential-based attacks to a large extent.

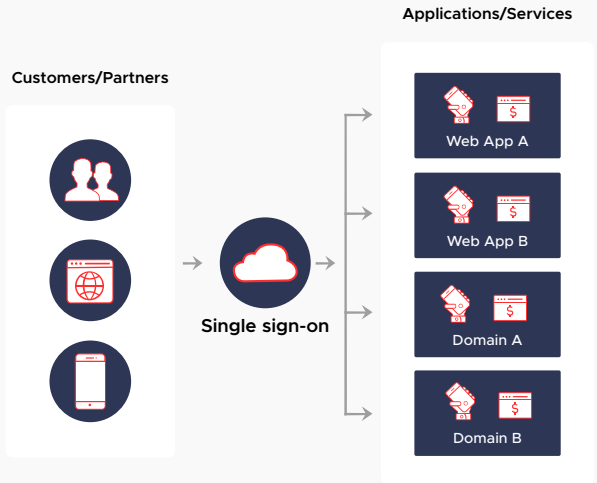


Single sign-on

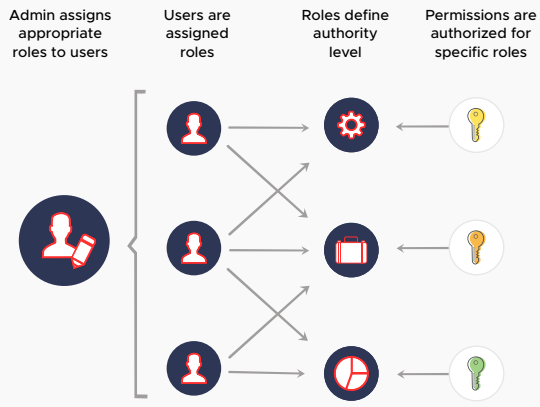
Single sign-on (SSO) enables users to verify themselves using a single set of credentials to gain access to multiple applications or systems. This eliminates the need for users to log in separately for each system. For example, by signing in to a single Google account, you can access multiple services such as Gmail, Google Docs, and YouTube. Since users need only a single set of login credentials, the number of passwords is reduced, which in turn reduces the attack surface. SSO also helps save time and energy and provides a streamlined experience to users.

Role-based access control

In role-based access control (RBAC), a predefined set of access privileges is granted for specific roles. For example, organizations typically provide elevated privileges to managers and the least amount of privilege to interns using RBAC. In other words, role-based access control is a means to implement the principle of least privilege. This is particularly useful for large organizations that contain thousands of employees and hundreds of different roles and permissions. Users are given access to resources on a need-to-know basis, which reduces their exposure to the sensitive and critical parts of the network. This helps reduce the number of security breaches and data thefts and enhances network security.



Single sign-on



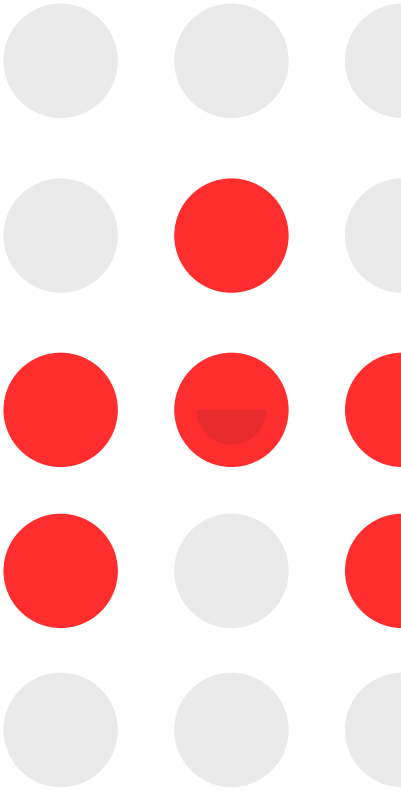
Role-based access control

The evolution of IAM

Identity and access management was prevalent long before the invention of computers and the internet. Prior to the advent of computers, identity and access were managed manually by humans. People proved their identities using their name or other credentials such as their birth certificate, passport, or driver's license. Access control was performed manually with the help of gatekeepers. The first digital identities and passwords were created in the 1960s with the development of networked computing. This included usernames and passwords as authentication factors while authorization was carried out using manual spreadsheets and access control lists. Network firewalls were used until the 1990s to secure the information and resources of an organization.

With the growth of the internet in the 1990s, traditional identity management systems were switched out in favor of online applications, which automated some of the manual tasks. However, in the early 2000s, the exponential growth in the number of internet users led to an increase in the number of data breaches and fraudulent activities. This in turn caused the Sarbanes-Oxley Act (SOX), which demanded tighter security and increased identity management, to be passed in 2006 by the United States government.

The later years saw a tremendous increase in the advancement of IAM systems, which employed MFA, SSO, privileged access management, and biometrics. At present, the growth of IAM technology is driven by trends such as distributed systems, decentralized identities, bring your own device (BYOD) policies, cloud adoption, the Internet of Things, Zero Trust, and passwordless authentication systems. IAM systems in the future are predicted to be based on biometric authentication, AI, and machine learning, indicating that the advancement of IAM systems and policies is inevitable to actively combat security threats.



The impact of the COVID-19 pandemic on IAM and cybersecurity

The onslaught of the COVID-19 pandemic brought about widespread disruption in cybersecurity operations all over the globe. Cyberattacks and data breaches reached an all-time high, leading to what many called a cyber pandemic. As organizations adopted remote work, the security perimeter was no longer confined to the organization, which threatened to increase the rate of cyberattacks and threats.

Organizations all over the world are gradually opening their office spaces to their employees, making the hybrid workforce model indispensable. Simply put, a hybrid workforce model is a blend of the in-office and remote working models. This hybrid model is all set to become the new normal, considering the benefits it offers in terms of flexibility, productivity, and cost-effectiveness. Since employees are constantly migrating between their remote and in-office working spaces, this model is highly vulnerable to cyber threats and attacks. Current cybersecurity and IAM standards need to be revised in order to support a workforce that's constantly on the move.

Another factor is the lack of resources to handle the sudden increase in teleworkers. This has left many organizations vulnerable to malware and phishing attacks, many of them COVID-19 themed. Since IAM plays an important role in the overall IT security of an organization, these factors have a considerable impact on identity and access management costs and trends.

There's been a shift towards alternative contactless biometric solutions, such as iris and facial recognition, as opposed to fingerprints. IAM systems in the future might be required to implement touchless or contactless biometric solutions for identification and authentication. Additionally, behavior detection, body recognition, and other advanced technologies should be considered to identify and authenticate users.

Organizations are rapidly transitioning towards cloud computing environments to improve their IT operations. While cloud adoption offers many advantages such as increased computing power, storage, scalability, flexibility, and cost efficiency, it also holds potential risks to the security of the organization. Cloud environments are typically more vulnerable to cyberattacks due to limited visibility of resources, the need for authentication, and a lack of auditing.

This requires stringent access management systems as ineffective security systems can cause data breaches and leaks.Access to the cloud can be controlled and managed by deploying IAM techniques such as MFA. Inevitably, an increase in IAM spending is required to secure and manage cloud identities and resources.

Due to the increased number of cyberattacks during the pandemic, many organizations suffered massive losses in revenue. The increase in the number of cyberattacks leads to a corresponding increase in the cost of data breaches. The cost and occurrence of data breaches is expected to increase further in the coming years. This calls for organizations to increase their budgets for robust IAM systems and to ramp up the overall security.

IAM future trends and roadmap

Cybersecurity mesh

According to a report by Gartner, the cybersecurity mesh model is predicted to support more than 50% of IAM requests by the year 2025. One of the biggest changes brought about by the COVID-19 pandemic is widespread remote working, which requires organizational assets to exist outside the traditional security perimeter. With employees, clients, and vendors being located in various distributed regions, the security perimeter also has to extend to these regions. As a result, security threats and attacks are increased. This problem can be addressed by the cybersecurity mesh model, which proves to be the most practical approach for managing and providing access to resources, devices, and users located outside the security boundary.

The cybersecurity mesh model is a distributed architectural approach in which the security perimeter is built around the identities of people or objects, enabling security control to be scalable, flexible, and reliable. The traditional security model, known as the castle-and-moat approach, relies on strong perimeters constructed of firewalls to keep out attackers and malicious actors. In other words, everything inside the network perimeter is considered safe while everything outside is considered dangerous. The internal network is trusted by default, which in turn increases the risk of other types of threats such as insider threats.

However, these types of threats are considered to be among the most significant risks to the security of an organization. The goal of this model is to ensure that the security of each access point is managed from a centralized point of authority.

The cybersecurity mesh acts as a building block of the Zero Trust approach of security. The Zero Trust approach is based on the principle of "never trust, always verify." This ensures that no user or device is trusted, regardless of whether they're located within or outside the network. With the principle of Zero Trust, the security of an organization is improved as it is no longer based on the traditional network perimeter approach. A cybersecurity mesh thus aids in implementing a Zero Trust architecture by ensuring that all users and devices are verified before being allowed access to the network.

50%

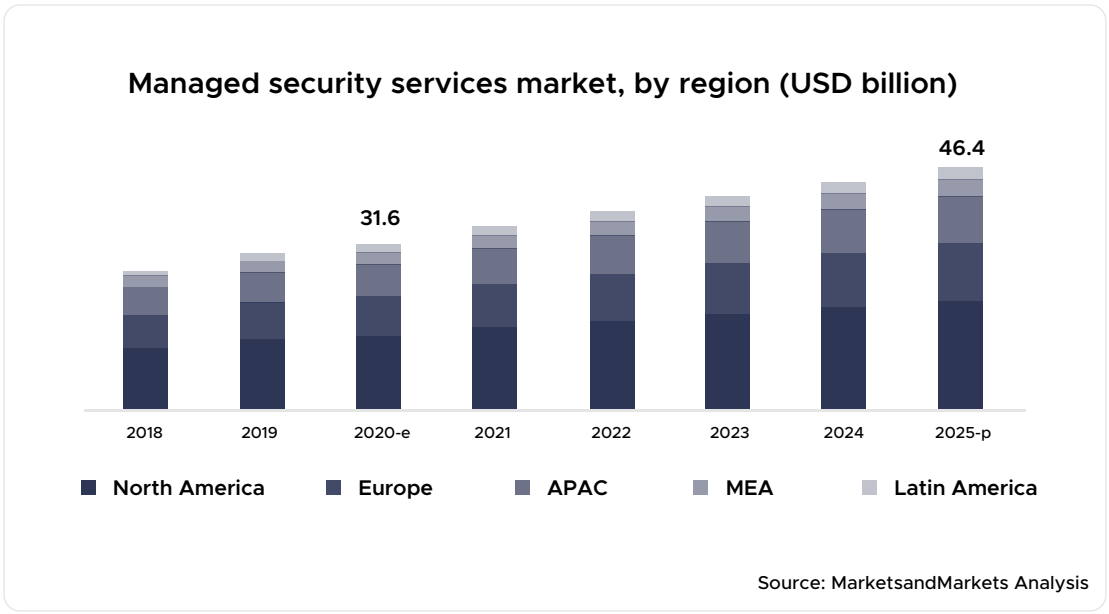
of IAM requests by 2025 will be supported by cybersecurity mesh.

- Gartner

Managed security service providers

The overwhelming rise in the number of cyberattacks and data breaches has seen IT firms receiving an increase in the number of cybersecurity-related enquiries. Clients require assistance in managing the remote workforce, assessing the security of the organization, and defending their networks against potential cyberattacks. In other words, demand is increasing for cybersecurity services as organizations struggle to keep up against the continuously evolving cyberthreat landscape. They also lack the necessary skills and resources to develop and implement competent identity and access management systems, and instead employ professional service providers known as managed security service providers (MSSPs). Gartner has predicted that the delivery of IAM services will increase through MSSPs, such that 40% of IAM application convergence will be driven by MSSPs by the year 2023. These service providers focus on providing best-of-breed solutions with an integrated approach.

A managed security service provider provides security services to organizations, including the deployment and maintenance of firewalls, VPNs, antivirus systems, and IAM systems. They may serve as an extension of the IT department of an organization by taking up all or some aspects of the IT security functions. MSSPs are also comparatively more cost-effective than hiring and training the in-house security team. According to a recent report by MarketsandMarkets, the global managed security services market is predicted to reach $46.4 billion by the year 2025 due to increasing demand for MSSPs. Identity and access management systems can be made more effective and efficient by outsourcing them to MSSPs. This doesn't only apply to large-scale organizations; as security threats and data breaches continue to increase, small and medium-sized businesses can also benefit from these service providers.



Source: MarketsandMarkets Analysis

Identity proofing tools

The adoption of online services ranging from video conferencing to online healthcare has gained momentum during the COVID-19 pandemic. This has created an increase in the demand for the verification of digital identities, with the help of identity proofing. Since organizations are liable to suffer huge losses at the hands of identity-related attacks, data breaches, identity fraud, and thefts, it's crucial for them to fortify their identity verification processes. This can be performed with the help of identity proofing tools. According to a Gartner report, identity proofing tools will be implemented by 30% of large enterprises within the workforce identity life cycle by the year 2024.

Identity proofing is the process by which a user's association with their real-world identity is verified in order to prevent unauthorized access. In simpler terms, identity proofing verifies whether the user's claimed identity matches their actual identity. The verification is done based on the user's life history, biometrics, or other publicly available data. Traditionally, user identities involved verifying the username and password, which are usually self-registered. This is very basic and does not offer much protection against cyberattacks. It is therefore crucial to add an additional layer of authentication and security by verifying the user's identity based on their biometrics, physical identification documents, knowledge-based security questions, or other similar authentication factors.

According to the Digital Identity Guidelines published by the National Institute of Standards and Technology (NIST), there are three steps that are crucial to the identity proofing process. These steps are as follows:

Resolution:

The process by which a user's identity is uniquely distinguished in the context of the system.

Validation:

The process by which evidence or proof is collected from the user and checked to ensure that it is authentic and valid.

Verification:

The process by which the claimed identity of the user is verified to be true.

With the help of identity proofing tools, all these operations can be performed automatically to ensure that only trusted users are given access to the network resources. It also ensures that the occurrences of identity theft and fraud are prevented and curbs the increase in cyberattacks and unauthorized access. In order to improve their security and reduce IAM-related issues, it's important for large organizations to seek the help of identity proofing vendors as part of their IAM solution.

Decentralized identity standards

The traditional method of centralized identity management has many shortcomings owing to the lack of privacy, security, and pseudonymity. Gartner has predicted that a global, portable, decentralized identity standard will emerge by the year 2024 to deal with different use cases. Blockchain technology can be used to implement a decentralized approach, which helps overcome the shortcomings of the centralized approach to identity management. By employing a decentralized approach, an individual's privacy is protected since only the minimal required information needs to be provided. This is in contrast to the current methods, where the individual generally has to provide additional information which is not actually required for authentication. This raises issues regarding the privacy, security, and data protection of an individual. Additionally, using a centralized system for identity management increases the risk of cyberattacks and data breaches by providing a single target point for hackers.

> In the decentralized approach using blockchain, identity management is based on a user-centric model. This means that the user can control and manage their identity data without having to interact with intermediaries.

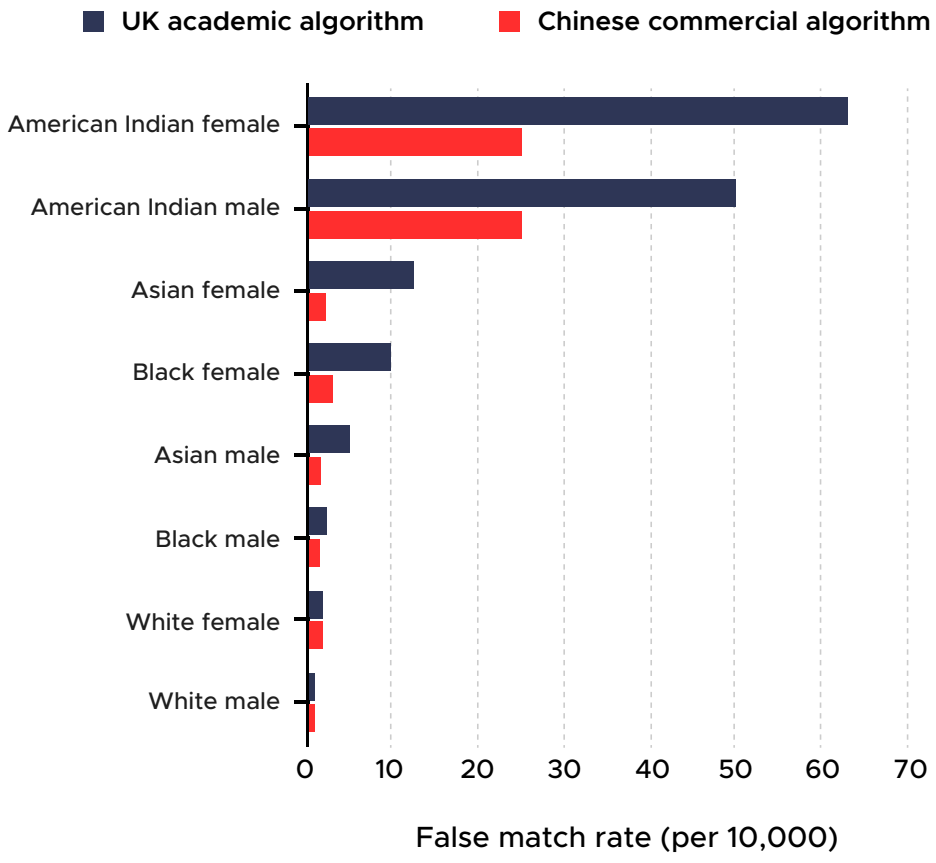
Blockchain technology, also known as distributed ledger technology, is a decentralized database that is managed by multiple participants in a peer-to-peer network. The information is recorded in blocks, after which it is duplicated and distributed to all members in the network. Every member in the network has a ledger of all the transactions—which means that every transaction is immutable, transparent, and secure. It's one of the three pillars of self-sovereign identity (SSI), where the users can store their identity on their own devices and choose the pieces of information they want to share with verifiers. The decentralized identifiers (DIDs) can be used for enabling a verifiable and decentralized digital identity. They can be used to identify any type of subject and to create a private, secure, peer-to-peer connection between two entities.

The zero-knowledge proof system is an encryption scheme that can be implemented in blockchain technology for a decentralized identity management system, which doesn't store any personal information on its users. By employing a zero-knowledge proof system, the user can provide authentication factors without disclosing the actual information used to support the proof. The actual data is not revealed to the verifier, which in turn protects the privacy of the user. Self-sovereign identities based on blockchain technology can be used to overcome the challenges in privacy, security, and pseudonymity faced while using centralized and federated identity management systems. The blockchain market is expected to reach $60 million by 2024, which makes it one of the most popular technologies to be adopted for identity and access management.

Minimizing demographic bias in identity proofing

The use of facial recognition for document-centric identity proofing experienced a rapid expansion in 2020 as a result of the increase in online use cases. This method involves comparing a selfie of the customer with the photograph in their identity document for verification. The facial recognition algorithms used for this purpose are found to exhibit a demographic bias against different ethnic groups, age groups, genders, and other factors which include camera or device quality. For example, in a study conducted by NIST, it was discovered that African American and Asian faces were falsely identified 10 to 100 times more when compared to Caucasian faces. Besides affecting the accuracy of recognition, it also has potential risks relating to customer relationships and experience, brand damage, and legal implications. This requires identity proofing vendors to minimize demographic bias and provide evidence of doing so.

Comparison of false positive rates among different facial recognition algorithms



Gartner has stated that by the year 2022, 95% of organizations will have to demand that their identity proofing vendors prove that they are minimizing demographic bias, which is an increase from the current 15%. With regard to this, Jumio has issued five practical ways to check AI bias in online identity verification. These are as follows:

- The training database should be large and needs to represent a wide range of samples. This is to ensure that the machine learning (ML) model is trained to recognize different types of data and make relatively accurate predictions. Using a larger and more representative data set helps make sure the system isn't biased. For instance, facial recognition and authentication models must be trained using images of people belonging to a wide range of age groups, genders, nationalities, ethnicities, and socioeconomic backgrounds.

- ML models should be trained using real-world data sets. Organizations often use third-party data sources when they're running short on data; these data sets usually contain images that are obtained under perfect lighting conditions with good camera resolution. However, this may not always be the case when dealing with real-world images, which are captured under dim lighting conditions with poor camera resolution. This introduces a bias in the algorithm, as it will not be able to recognize images with real-world imperfections. Hence, AI models must be built and trained on realistic data sets to avoid demographic bias.

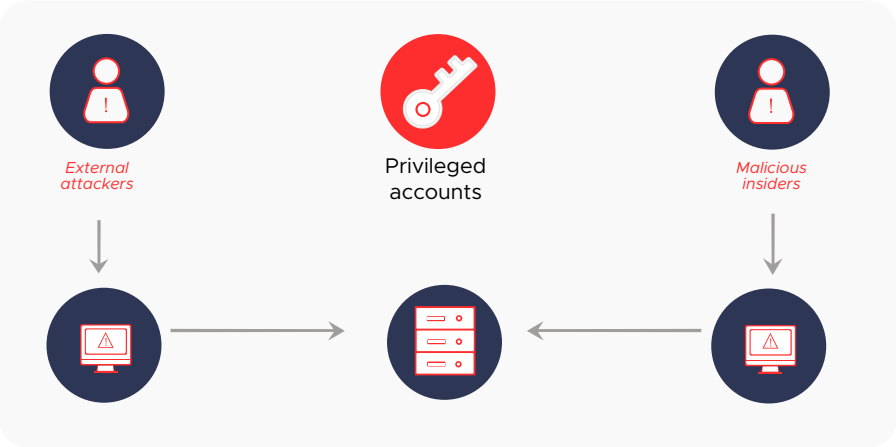
- The data set should be tagged properly to represent the characteristics of the images that are used. This is especially important in identity verification for detecting fraudulent identities. Images with poor lighting, blur, or glare must be labeled to denote those features. This ensures that the resultant model can recognize and verify identities with accuracy.

- The tagging process must be carried out with proper quality control in place. This is to ensure that the process is performed by specialists and with accuracy, helping the model be less biased and more accurate.

- The team that develops the algorithm must be composed of members belonging to different genders, nationalities, professional experiences, and academic backgrounds. The diversity in the team makes sure that there are different perspectives while developing the model. This in turn helps in reducing the demographic bias exhibited after deployment.

Privileged access management

Privileged access management (PAM) is composed of cybersecurity strategies and processes used to manage and secure access to elevated or privileged accounts in an organization. These accounts may include privileged users such as administrators, who typically have elevated access and permission to critical resources. These accounts are usually the target of cyberattacks, as gaining access to these accounts allows the attackers to access privileged and highly confidential information. In addition to this, privileged accounts have permission to make configuration changes at the administrative level and other critical permissions, so it's important to provide a high level of security to these accounts. This is done with the help of PAM, which is an integral part of identity and access management. The credentials of the privileged accounts are stored in a highly secure repository or vault, the access to which is managed by a PAM system.



Due to the increasing number of cyberattacks and data breaches, PAM is crucial to protect organizations from both outsider and insider threats. According to a recent report published by MarketsandMarkets, the privileged identity management market is predicted to reach a growth of $3792.5 million by 2021, compared to a record of $922 million in 2016 at a continuous annual growth rate of 32.7%. While traditional PAM systems relied on passwords for security, passwords are now considered insecure. Current and future PAM systems must aim at an identity-centric approach that's flexible and easy to deploy.

IAM for cloud services

The sudden surge in the number of remote workers at the onset of the pandemic led to a large number of organizations moving to the cloud. Gartner has predicted that by the year 2024, the cloud will account for 14.2% of total global enterprise IT spending, a significant increase from 9.1% in 2020. While cloud adoption offers many benefits such as scalability, flexibility, and efficiency, it also poses security threats due to limited visibility of resources, lack of auditing, and a need for authentication. This in turn requires a new range of policies to manage and monitor cloud identities effectively. Therefore, deploying a stringent identity and access management system is critical to protect the cloud environment from security breaches and threats.

Conclusion

The increasing sophistication and complexity of identity-related attacks emphasizes the need for organizations to deploy competent IAM systems and to keep up with the future trends in the field. Additionally, the consequences brought about by the COVID-19 pandemic contribute to significant changes in identity and access management approaches. Remote working and BYOD policies have redefined the traditional security perimeter. There is also consistent acceleration towards digitization and adoption of cloud services, and in turn demand for more flexible and granular policies to accommodate for the constantly evolving IAM landscape.

Technologies such as Zero Trust, identity analytics, user behavior analytics, ML, AI, and decentralized identity standards are expected to become more prevalent in the coming years to overcome the inadequacies of traditional IAM solutions. Similarly, to cater to the needs of the remote workforce, organizations are anticipated to rely more on managed security service providers and identity proofing vendors and tools to manage their IAM and cybersecurity needs. Identity proofing vendors need to minimize demographic biases against individuals belonging to different nationalities, genders, and ethnic groups, and IAM policies and systems should focus on adapting to the changing landscape and take various parameters into consideration. They should be efficient, scalable, flexible, and cost-effective while taking into account current and future market trends.