International Journal of Engineering & Technology, 12 (1) (2023) 11-14

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Identity and access management: "Elevating security and efficiency: Unveiling the crucial aspects of identity and access management"

Saloni Kumari *

Software Engineer II at EY (Ernst & Young), Hyderabad, India
**Corresponding author E-mail: salonisingh899@gmail.com*

Abstract

The foundation of the software is the identity and access management system. A fundamental and essential cybersecurity competency is ensuring that the right parties have timely access to the right resources. The IAM has four domains: IAAA stands for identification, authentication, authorization, and accounting, the second is Privileged Access Management (PAM), third-party Identity Governance and Administration, data governance and protection. In this article, the concepts of identification, authentication, authorization, and accounting are discussed, as well as how IAAA works in an online setting.

Keywords: *Authorization policies; Security best practices; User Authentication; Digital identity; Data security; IAM framework; Role-based access control; Access management strategies; Cybersecurity compliance; User accountability; Access control mechanisms.*

1. Introduction

IAM is a framework of rules, procedures, and tools that enables businesses to govern user access to sensitive corporate data and digital identities. IAM enhances security and user experience, enables better business outcomes, and boosts the viability of mobile and remote working as well as cloud adoption by assigning users with specific roles and ensuring they have the proper level of access to company resources and networks.
Only one specific class of resource-based policy, known as a role trust policy and associated to an IAM role, is supported by the IAM service. An IAM role enables resource-based policies by acting as both a resource and an identity. Because of this, you must give an IAM role both a trust policy and an identity-based policy.

2. Research methodology

2.1. CIA principles

Information is safeguarded against unauthorized access and misuse by confidentiality procedures. Most information systems contain sensitive information to some extent. It could be confidential corporate information that rivals could exploit or private data pertaining to staff, clients, or consumers of a company. Organizations take a variety of preventative actions to guarantee anonymity. To restrict access to resources, software is used along with passwords, access control lists, and authentication methods. To safeguard data that can still be accessed despite the controls, including emails that are in transit, encryption is used in addition to these access control mechanisms. Physical controls that restrict access to facilities and equipment are another form of confidentiality protection, as are administrative measures like policies and training.
Information is shielded from unauthorized tampering by integrity safeguards. These procedures guarantee that the data are accurate and comprehensive. Information must be protected both when it is stored on computers and when it is transferred between systems, like during email. To guarantee integrity, it is vital to not only restrict access at the system level but also to make sure that users of the system can only make changes to the data that they have been given permission to make. Authorized users can be stopped from making unauthorized changes with access control and strict authentication. Digital signatures and hash verification can help guarantee the integrity of files and the authenticity of transactions. Administrative controls like duty separation are equally crucial to preserving data integrity.
A system of information must be usable for authorized people to access it. Access to the system is protected from disruptions by availability safeguards. Hardware failures, unplanned software outages, and network bandwidth problems are some of the non-malicious types of risks that are the most essential to availability. Various sabotage tactics used in malicious assaults aim to hurt a company by preventing people from accessing its information system. As diverse as the challenges to availability are the availability countermeasures to protect system

Copyright © Saloni Kumari. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

availability. High-availability systems should have a lot of hardware redundancy, with backup servers and data storage always available. It is typical for large enterprise systems to have redundant systems in several physical locations.

2.2. IAAA concepts

The access management process's last four components are identification, authentication, authorisation, and accountability.
To govern and secure access to systems and resources, access management is a crucial component of information security. Identification, Authentication, Authorization, and Accountability, also known as the "Four A's," are four core components that are crucial to the access management process.

1) Identification:

The process of access management begins with identification. To claim an identity within a system or organization, a user must provide a special identifier, such as a username, email address, or employee ID. The identifier acts as the initial piece of information that a system needs to identify and separate the user from other users. However, it only links a label or name with a possible user; it does not create trust or validate the user's identity.

2) Authentication

The process of certifying that a user or entity is who they say they are and hence validating their claimed identity is known as authentication. It confirms that the user has legitimate identification to back up their stated identity, such as a password, biometric information, or cryptographic keys. Creating trust in the user's identity is the aim of authentication. To confirm their identity, users frequently have to present something they have (like a smart card or smartphone), something they know (like a password), or something they are (like a fingerprint or retina scan). Strong authentication techniques that demand numerous forms of verification, such two-factor authentication (2FA) or multi-factor authentication (MFA), improve security.

3) Authorization:

Authorization is used once a user's identity has been satisfactorily verified. A user's access to certain actions or resources inside a system or organization is determined by their authorization. Administrators establish authorization rules and policies that outline the user's privileges, roles, and permissions based on their identity and characteristics. What is permitted or prohibited is decided by these regulations.
By requiring authorization, users can only access resources and carry out tasks that are pertinent to their roles and responsibilities. It shields sensitive information and stops unauthorized actions.

4) Accountability

Accountability is the component that makes sure user actions within a system or organization can be tracked back to and linked to certain people or entities. It entails recording and auditing human actions and system events. These logs record details such as who accessed what, when, and how actions were taken. Accountability is essential for compliance and security reasons. Accountability logs assist in locating the issue's origin and assigning blame in the event of security incidents, breaches, or compliance audits. Since users are aware that their actions are being tracked and recorded, accountability also serves as a deterrent against malevolent behaviour.

In conclusion, identification, authentication, authorization, and accountability, the four components of the access management process, cooperate to make sure that only authorized users have access to the right resources and that their actions are tracked and traceable. This all-encompassing strategy aids firms in upholding the security, compliance, and integrity of their information systems and surroundings.

2.3. Identity federation

Users can access numerous apps or services across various organizations or domains via the identity federation technique, which uses a single set of credentials or identity. It permits the easy exchange of user identity and authentication data across reliable parties, often without the need to set up unique accounts and passwords for every service. Identity federation, a major element of contemporary identity and access management (IAM) systems, is essential for boosting user ease, security, and interoperability.
Here are the key components and principles of identity federation:

Single Sign-On (SSO) in identity federation makes Single Sign-On possible, which allows users to log into their primary identity provider (IdP) once to access different applications or services without having to repeatedly enter their credentials. As a result, managing several usernames and passwords is easier for users and the user experience is streamlined. IdPs, or identity providers in identity federation, one or more identity providers serve as reliable sources for user identity data and authentication. IdPs validate user identities and offer tokens or assertions (such Security Assertion Markup Language - SAML or OAuth tokens) that confirm the user's identity and authentication status. Applications, services, or resources that users seek access to are known as service providers (SPs). Instead of managing user authentication themselves, SPs use the assertions made by the identity provider to provide access and rely on the identity provider to authenticate users. Identity federation depends on the existence of trust connections between IdPs and SPs. The claims made by the IdP, and the user's identification information must be trusted by SPs. Usually, certificates and cryptographic keys are used to establish this confidence. Standards and Protocols enable the exchange of identity information and authentication tokens between IdPs and SPs, identity federation makes use of industry-standard protocols and formats, such as SAML (Security Assertion Markup Language), OAuth (Open Authorization), OpenID Connect, and WS-Federation. Identity federation not only authenticates users but also permits the sharing of other user attributes (such as name, email address, and role) with SPs in accordance with user authorization and consent standards. Due to this, SPs can tailor the user experience based on user traits. Identity federation is particularly helpful in situations when users must have access to resources or services provided by various organizations, such as in partnerships, collaborations, or cloud-based services. Users can seamlessly access resources in another company while still retaining security and control.

Benefits of identity federation include:

- User experience is improved since SSO makes it easier for users to remember only one username and password instead of having to remember several.
- Enhanced Security: By enforcing strict access controls and centralized authentication standards at the IdP, security can be made more secure.
- Administration Simplified: Organizations can centralize user management to cut down on the administrative burden of maintaining user accounts across many systems.

- Identity federation encourages interoperability between various systems and domains, giving smooth access to resources without the need for time-consuming integration procedures.
- Compliance: By establishing uniform access controls and audit trails, federation can assist in achieving compliance standards.

2.4. Single sign-on (SSO)

After logging in just once, a user can access various apps or services using a single set of credentials (such as a username and password). This authentication method is known as single sign-on. SSO's main objective is to make using software easier by eliminating the need for users to remember and enter numerous usernames and passwords for various apps.
Here is how SSO functions:

- User authentication occurs when a user enters their credentials to access an SSO-enabled system (often known as the Identity Provider, or IdP). Their identity is confirmed by the IdP.
- Access to a Variety of Services: The IdP sends a token or session cookie after authentication so that the user doesn't have to enter their credentials again while using other services or apps (Service Providers or SPs).
- Access Control: The SP depends on the IdP to verify the user's identity since it has faith in it. The user obtains access to the SP without having to log in again if the token is legitimate.
- SAML (Security Assertion Markup Language), OpenID Connect, and WS-Federation are important SSO protocols. SSO is frequently used in business settings and web applications to increase user comfort and security.

2.5. OAuth (open authorization)

With the help of the OAuth permission framework, applications can access a user's resources on a different service without disclosing or sharing the user's login information. OAuth, in contrast to SSO, is typically used to offer restricted access to a user's data or functionality to third-party applications (such as social media data or email contacts) without divulging the user's password.
Here is how OAuth functions:

- Resource Owner: The user (the resource owner) authorizes a client application to access resources on a resource server (such as a social media server) without disclosing their login information.
- Authorization Server: The authorization server, frequently run by the service provider, verifies user identity, and provides the client with an access token.
- When requesting access to a user's resources, the client must give the access token to the resource server. The resource server validates the token's legitimacy before granting access.
- OAuth is frequently used in situations where a user wants to grant temporary or restricted access to their data to a third-party application without disclosing their login credentials. Social networking logins and API access to internet services are examples of frequent use cases.

2.6. Authentication methods

Authentication is the process of verifying the identity of a user or system to ensure that they are who they claim to be before granting access to a resource, such as a computer system, online account, or physical facility. Different methods of authentication exist, ranging from basic to more secure approaches. Single Factor Authentication (SFA), Two-Factor Authentication (2FA), and Multi-Factor Authentication (MFA) are three common methods, each offering different levels of security.

1) Primary/Single-Factor Authentication

Single Factor Authentication is the simplest and least secure form of authentication. It relies on just one factor to verify a user's identity. Typically, this factor is something the user knows, such as a password or PIN. When a user enters their password, the system checks it against the stored password and grants access if the entered password matches the stored one.
Pros:
Simplicity: Easy to implement and use.
Low cost: Requires minimal infrastructure.
Cons:
Vulnerable to attacks: SFA is susceptible to various security threats, including password guessing, phishing, and credential theft.
Lack of robustness: If the single factor (e.g., a password) is compromised, unauthorized access can occur.

2) Two-Factor Authentication

Two-Factor By requiring two distinct factors for user verification, authentication offers an extra degree of protection. The three main sorts of factors are as follows:

a) A secret phrase or password that you know.
b) A piece of property you own, like a smartphone or hardware token.
c) A part of you (like biometric data like a fingerprint or facial recognition).

A user needs to supply two of these factors to authenticate. For instance, after entering a password (something you know), the system might send a one-time code to the user's smartphone (something you have), which the user must also enter to get access.
Pros:
Enhanced security: Since an attacker would have to compromise both factors, 2FA mitigates many of the vulnerabilities associated with SFA. Reduced danger of illegal access: If one element is compromised (for example, a password is taken), the second factor still prevents access.
Cons:
A little more challenging for users uses a hardware token or smartphone as the second authentication factor, which users must own and manage.

3) Multi-Factor Authentication

Multi-Factor Authentication is an improved form of 2FA that includes one or more extra factors in addition to the first two. MFA integrates elements from the three categories—something you know, something you have, and something you are—mentioned before. For instance,

to authenticate, a user might be required to provide a password (something you know), have their fingerprints taken (something you are), and enter a one-time code from their smartphone (something they have).
Pros:
Most advanced level of security provides the best security against illegal access.
Versatility: Enables companies to select a set of elements that best meets their security requirements.
Cons: It's more difficult for users: Due of the requirement for several elements, it could be less user-friendly.
Higher implementation costs possible maybe requiring new infrastructure in terms of hardware or software.
In many applications, MFA is regarded as the gold standard for security, particularly when it comes to safeguarding sensitive data or systems. It comes highly recommended for accounts and systems where security is of the utmost importance because it significantly lowers the chance of unwanted access.

3. Results and discussion

The key ideas of Identity and Access Management (IAM) and its four main domains, Identification, Authentication, Authorization, and Accounting (IAAA) have been examined in depth. We have talked about IAM's importance in the context of cybersecurity, emphasizing how it protects sensitive information and improves user experiences. We also looked at the CIA principles (Confidentiality, Integrity, and Availability) in relation to IAM, highlighting how crucial it is to uphold these standards in access management. Additionally, we have expanded on the IAAA ideas by offering explanations of how Identification, Authentication, Authorization, and Accountability work together to create the basis of a solid IAM approach. We've emphasized the differences between these components, highlighting that whereas Identification relies on information that is publicly available, such as usernames, Authentication relies on human knowledge, possession, or being. While Accountability makes ensuring that actions are recorded and linked to specific people, Authorization establishes what actions users are allowed to carry out. Identity Federation and Single Sign-On (SSO) have also been discussed as IAM techniques in the study, giving light on their functions in simplifying access control and management. The growing security levels offered by authentication techniques like Single-Factor, Two-Factor, and Multi-Factor Authentication were also highlighted. Overall, this paper gives a thorough explanation of IAM and its core elements, highlighting the significance of each for upholding a secure and effective digital environment. To safeguard their assets and user data while enabling easy access for authorized users, it highlights the necessity for enterprises to adopt comprehensive IAM processes.

4. Conclusion

To sum up, Identity and Access Management (IAM) is a crucial component of contemporary cybersecurity and is necessary for protecting sensitive information, guaranteeing the reliability of systems, and preserving resource availability. From the fundamental ideas of Identification, Authentication, Authorization, and Accountability (IAAA) through the tenets of Confidentiality, Integrity, and Availability (CIA), this essay has carefully examined the major components of IAM. It has clarified the important differences between these elements and stressed the importance of each in the context of access management. A strong IAM framework is not an option but rather a necessity in the modern digital environment, where threats from data breaches and illegal access are constantly growing. IAM techniques must be proactively implemented by organizations in order to strengthen their cybersecurity posture, manage risks, and guarantee regulatory compliance. By doing this, they not only safeguard their valuable assets but also allow authorized individuals to access them securely and quickly, eventually enhancing public trust in their online business operations. IAM will continue to play a crucial role in protecting the digital world as technology develops, making it an essential area of attention for businesses looking to prosper in a more linked and data-driven environment.

Acknowledgement

I would like to offer our deep appreciation to my company EY (Ernst & Young) for their constant support, important advice, and encouragement throughout our journey. Their insightful suggestions and helpful criticism considerably raised the caliber of this investigation. I want to thank my friends and research colleagues for their contributions, as well as for their insightful comments, lively debates, and helpful criticism. Their varied viewpoints substantially improved this work.

References

[1] Kling J, Thompson B, Green W. IAM System Implementing Iam Data Model. US Patent 9. 2016: 529-989.
[2] Hardt D. (2021) RFC6749—The OAuth 2.0 Authorization Framework. https://tools.ietf.org/html/rfc6749. Accessed February 18, 2021.
[3] Hu VC, Ferraiolo D, Kuhn R, et al. Guide to attribute-based access control (abac) definition and considerations. NIST Special Publ. 2013; 800(162): 4-16. https://doi.org/10.6028/NIST.SP.800-162.
[4] Vimercati DC, Foresti DC, Samarati SP. Authorization and access control. In: Security, Privacy, and Trust in Modern Data Management. Berlin: Springer Berlin Heidelberg; 2007: 39-53 https://doi.org/10.1007/978-3-540-69861-6_4.
[5] Nuss M, Puchta A, Kunz M. Towards Blockchain-based identity and access management for Internet of Things in enterprises. Intern Conf Trust and Priv Digital Bus. 2018: 167-181. Accessed February 18, 2021. https://doi.org/10.1007/978-3-319-98385-1_12.
[6] Osmanoglu E. Identity and Access Management: Business Performance Through Connected Intelligence. Newnes; 2013.
[7] Ghaffari F, Bertin E, Hatin J, Crespi N. Authentication and access control based on distributed ledger technology: a survey. 2nd Con Blockchain Res App Inno Net Ser (BRAINS). Paris, France; 2020: 79-86. September 27, 2020. https://doi.org/10.1109/BRAINS49436.2020.9223297.
[8] Gilani K, Bertin E, Hatin J, Crespi N. A survey on Blockchain-based identity management and decentralized privacy for personal data. 2nd Con Blockchain Res App Inno Net Ser (BRAINS). Paris, France; 2020: 97-101. September 27, 2020. https://doi.org/10.1109/BRAINS49436.2020.9223312.
[9] Chadwick DW. Federated identity management. In: Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures. Berlin: Heidelberg: Springer Berlin Heidelberg; 2009: 96-120. https://doi.org/10.1007/978-3-642-03829-7_3.
[10] Clauβ S, Kesdogan D, Kölsch T. Privacy enhancing identity management: protection against re-identification and profiling. Proceedings of the 2005 workshop on Digital identity management. Seoul, Korea; 2005: 84-93. November 15, 2005. https://doi.org/10.1145/1102486.1102501.