Identity & Access Management (IAM)

Eugene Choi

April 2021

1 Introduction

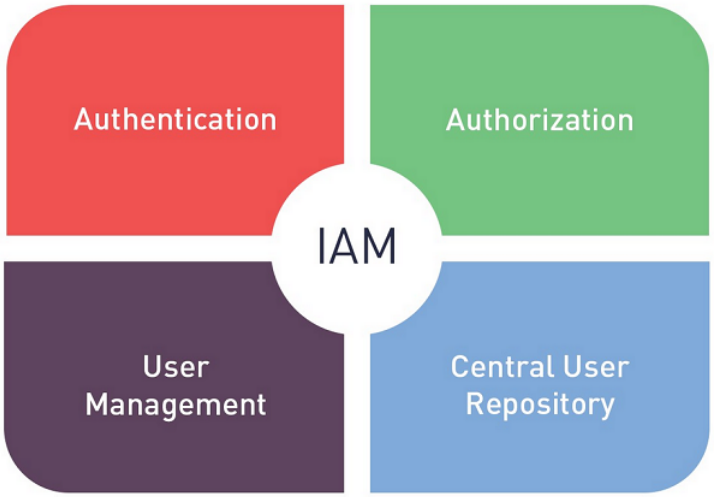
With cybersecurity being as crucial as ever in our increasingly data-driven world, protection of information is a must for all online businesses—small and large. Identity and Access Management, often referred to as IAM, is an integral part of business processes and structures that all cloud computing scientists should be familiar with. In a basic sense, IAM is the framework that facilitates the management of digital or electronic identities. Through IAM, business managers will be able to control the roles of individuals in a system and ensure security of data.

2 Components of IAM

At the fundamental level, IAM facilitates the following components:

- how individuals are identified in a system
- how roles are identified in a system and how they are assigned to individuals
- adding, removing and updating individuals and their roles in a system
- assigning levels of access to individuals or groups of individuals
- protecting the sensitive data within the system and securing the system itself

3 Fundamental Features



The four rectangles above represent key features of IAM. The top two rectangles, authentication and authorization, comprise access management, while the bottom two rectangles, user management and central user repository, comprise identity management. We will touch upon each of these concepts to get a better understanding of IAM.

3.1 Authentication

Commonly referred to as simply "logging in", authentication is the process of validating that people or entities are who they say they are.
Types of digital authentication include:

- **Unique passwords:** this is the most common type of digital authentication, and you are all likely familiar with it. Organizations will require longer or more complex passwords for better security.
- **Pre-shared key (PSK):** PSK is another type of digital authentication where the password is shared among users authorized to access the same resources (think of a branch office Wi-Fi password). This type of authentication is less secure than individual passwords.
- **Behavioral authentication:** this is more advanced than the other methods in that organizations use artificial intelligence to monitor user behavior. If this behavior deviates from the norm, they can automatically lock down systems.

Physical authentication is not as important in the field of cloud computing, but it can help get a better sense of what authentication encompass. Some examples include: retina, fingerprint, and face recognition.

3.2 Authorization

Authorization is the process of determining if a user has the right to access a service or perform an action. Users are granted authorizations according to their role at an organization.
Authorizations determine a role's resources and level of access in the network. These items may include systems, applications, file shares, and more. For example, a software engineer working on one project must be authorized to edit that part of the system. Authorizations are more complex than authentication and consist of numerous sets of rules, rights, groups, and permissions explicitly configured per user account.

3.3 User Management

User management defines the set of administrative functions such as identity creation, propagation, and maintenance of user identity and privileges. One of its components is user life cycle management which enables an enterprise to manage the lifespan of a user account. Self-service is a key concept within user management, and some examples of self-service include self-password resetting.

3.4 Central User Repository

The Central User Repository's main use is to store identity information. Additionally, it delivers identity information to other services, and provides service to verify credentials submitted from clients.

4 Benefits

IAM is crucial to protecting sensitive enterprise systems, assets, and information from unauthorized access or use. It also manages all users and employees in an organization; thus, it is an essential part of all businesses. Some benefits, aside from the obvious improvement to security, include:

- Increasing productivity by decreasing the total cost, repetitive tasks, and system downtime. IAM will take care of all authentication and authorization, and once roles are configured, roles can be simply added or removed to users.
- Companies that can properly manage identities have greater control of user access, which reduces the risk of internal and external data breaches.

- IAM systems help companies better comply with government regulations by allowing them to show corporate information is not being misused. The reliability of a company increases with the use of IAM.
- IAM provides a common platform for access and identity management information. This makes it easier to share data to clients and organizations in a protected network.

5 IAM in AWS, Azure, and GCP

IAM is provided on all three of the main cloud service providers as it is such a key element of businesses. IAM can be easily found in the control panels of AWS, Azure, and GCP as it is simply named "Identity and Access Management" across all three platforms.