EasyChair Preprint

№ 2495

# Securing Enterprise Information Using Identity Access Management

Sagar Kakade



January 29, 2020

# *Securing enterprise information using Identity Access Management*

Sagar Kakade
*IVS-FS*
*Infosys Ltd.*
Pune, India
sagarkakade7799@gmail.com

***Abstract*—Enterprise information in Identity and access management (IAM) solutions, has now moved to information protection from compliance. Industries are now aiming on Identity and access management solutions to improve enterprise information security. The objective of IAM systems is one digital identity per individual. The IAM basically consists of three main parts, Identity Management, Access Management and Identity Repository. Main objective is to achieve greater ROI and reduce total ownership cost.**

***Keywords—Access Management, Enterprise Information, IAM, Identity Management, ROI, Security, TCO***

## I. INTRODUCTION

In an enterprise IT organization, Identity and access management (IAM) is about defining and managing the roles and access privileges of individual. Access and management means circumstances in which users are granted/denied those privileges. Those users consist of customers or employees of organization. The main objective is to secure enterprise data through identity and access management which is than modified and monitored throughout each user's application access lifecycle [1]. To optimize efficiency, it is essential for the organization to be able to share enterprise information, resources, and applications with third parties in a secure manner. Identity access management (IAM) lays policies ensuring that the right person in an enterprise have the appropriate level access. IAM is complex business solution which includes entire enterprise such as organization's various unit, access points, locations of system, individual, partners and customers which is represented in below Fig.1. To verify identity and provide access to every individual in such diverse environment is very difficult and complex process.

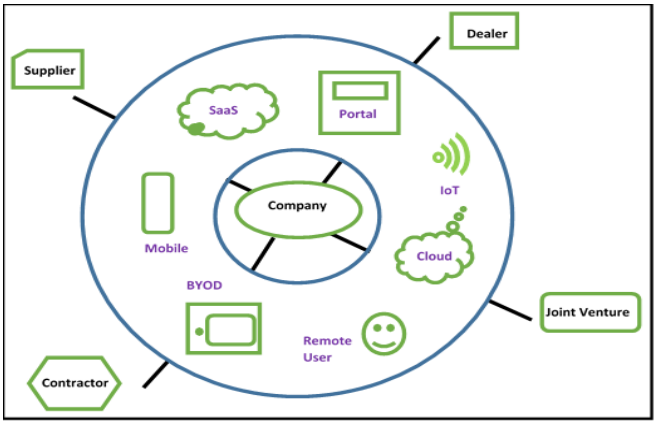


*Fig. 1: Distributed access to an organization*

## II. IDENTITY AND ACCESS MANAGEMENT TECHNOLOGIES

### *A. Repository Services*

Repository services are based on object oriented technology. Credentials of users are stored in repository that provide secure access to information [2]. Repository structure is hierarchical in nature which provide faster response to queries to identify the identity of an individual.

### *B. Identity Services*

Identity services include technologies designed to authorize and authenticate each user. These lifecycle includes creation of new user, alteration or modification of existing user, to synchronize user's date from various platforms, to revoke access to particular user.

Identity services is based on identity related monitoring of an individual with password management. It also manages to discard duplicate identity of an individual across various platforms. It also includes segregation of duties and reporting status management.

### *C. Access Service*

Access management services include services like managing access to various operating systems, application environments for end user. Access services allows the platform to record all the external user's information or to integrate with existing systems, synchronizing user profile and authorization information.

## III. PROVISIONING AND ONBOARDING APPLICATIONS

Onboarding and provisioning of applications has to follow certain set of policies such as technology implementation, segregation of duties and managing user accounts which is difficult business requirement. Organizations need robust approval-based access requests system which has the ability to audit access request. There are two main concerns of onboarding and provisioning.

### *A. Security of Information*

Organizations must prevent sensitive information from being accessed by unauthorized users. Unauthorized access to organizations critical information may lead financial loss, public embarrassment, or legal liability. With identity and access management capabilities, we can ensure only the right people have authorized access to the organizations information [2]. By centralization of security policy enforcement and controlling authentication and

authorization to its application infrastructure one can ensure security of organizations information.

### *B. Authorization and Access*

One must also be authorized (allowed) to complete his/her request. Authorization, uses the policies to determine whether to allow or deny the request. AWS technology uses JSON documents and specify the permissions for authenticate entities. There are various rules that can affect whether a request is authorized or not. To provide users with permissions to access the AWS resources in their own environment, one need only identity-based policies. Resource-based policies are popular for accessing cross-account access, i.e., access across various platform. AWS checks each policy that applies to the context of user request. If a single permissions policy includes a denied action, AWS denies the entire request and stops evaluating. This is called an *explicit deny* [2]. Because requests are *denied by default*, AWS authorizes your request only if every part of your request is allowed by the applicable permissions policies [2].

General rules for evaluation of request logic are as below:

- Requests that are made using the AWS account admin user credentials for resources in the account are always allowed. All the other request is denied by default.
- Default access can be overridden by explicit policies.
- An explicit deny in any policy overrides any allows.

## IV. Chanllenges or Risk of Implementing IAm

Security experts are concerned about integrating IAM with legacy systems (50 percent), moving to the cloud (44 percent) and unknown technology (43 percent) [3]. The concern now it to integrate existing systems with new IAM technology. The biggest challenge is that old practices that were put in place to secure legacy systems simply don't work with newer technologies. Implementation of identity and access management requires panning and collaboration across departments and cross platforms. An identity and access management system must be able to synchronize the user identity information across all these systems, providing a single source of identity of an individual. Manually providing access and controls for hundreds and thousands of users isn't possible in real-time. Also centralized operations is vulnerable target for hackers.

## V. Advantages of IAM

In today's world, most businesses need to give users outside the organization access to internal systems. Opening your network to customers, partners, suppliers, contractors and, of course, employees can increase efficiency and lower operating costs. Identity management can decrease the number IT support teams regarding password resets. Identity and access management systems allow root users to automate above mentioned and other time-consuming, costly tasks. An IAM system can be a heart of a secure network, because managing user identity is an important part of the access-control picture. An IAM system has defined access policies, specifically outlining who has access to which data resources and under which conditions they can access. Consequently, well-managed and maintained user identity mean greater control of user access, which helps to reduced risk of internal and external hacks. This is important because, along with the rising threats of external threats, internal attacks are all too frequent. Approximately 60 percent of all data breaches are caused by an organization's own employees, according to IBM's 2016 Cyber Security Intelligence Index. Of those, 75 percent were malicious in intent; 25 percent were accidental [4]. Thus the overall TCO is reduced using IAM and there is an increase in ROI.

## Acknowledgment

This information was supported by Infosys Ltd. I thank my colleagues who provided insight and expertise that greatly assisted the study, although they may not agree with all of the interpretations/conclusions of this paper.

## References

[1] OpenText, Secure Access to Enterprise Information with Identity and Access Management.

[2] Nilesh Shirke, Identity and Access Management

[3] CSO, What is IAM? Identity and access management

[4] IBM, Identity and Access Management Strategy and Assessment Services