

**CASE STUDY**

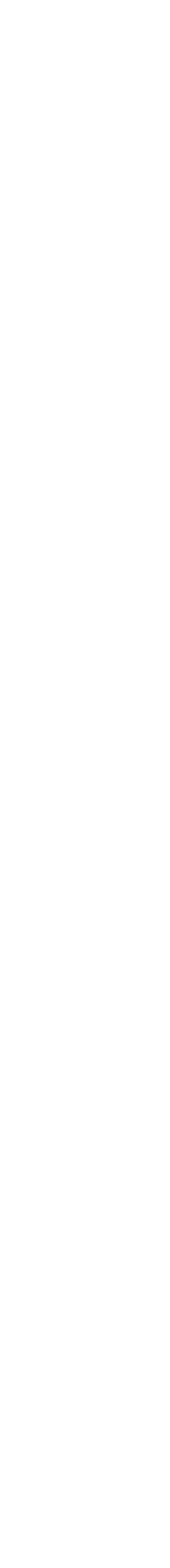
Designing a Robust Identity and Access Management (IAM) Solution for Enterprise Cloud Services

**SHUBHANGI SINGH 2141019345**

**Institute of Technical Education and Research**

**SIKSHA ‘O’ ANUSANDHAN DEEMED TO BE UNIVERSITY**

**Bhubaneswar, Odisha, India**



**INTRODUCTION**

Designing a robust Identity and Access Management (IAM) system is crucial for the security and efficiency of modern enterprises. In an era where digital transformation is reshaping industries, safeguarding sensitive information and ensuring proper access control is paramount. A well-architected IAM framework not only protects against unauthorized access and potential security breaches but also streamlines user management, enhances operational efficiency, and ensures compliance with regulatory requirements. By integrating advanced authentication methods, precise authorization protocols, and comprehensive auditing mechanisms, organizations can create a resilient IAM system that supports their business objectives while mitigating risks. This paper explores the essential components and best practices for developing a robust IAM strategy that meets the dynamic needs of today's digital landscape.

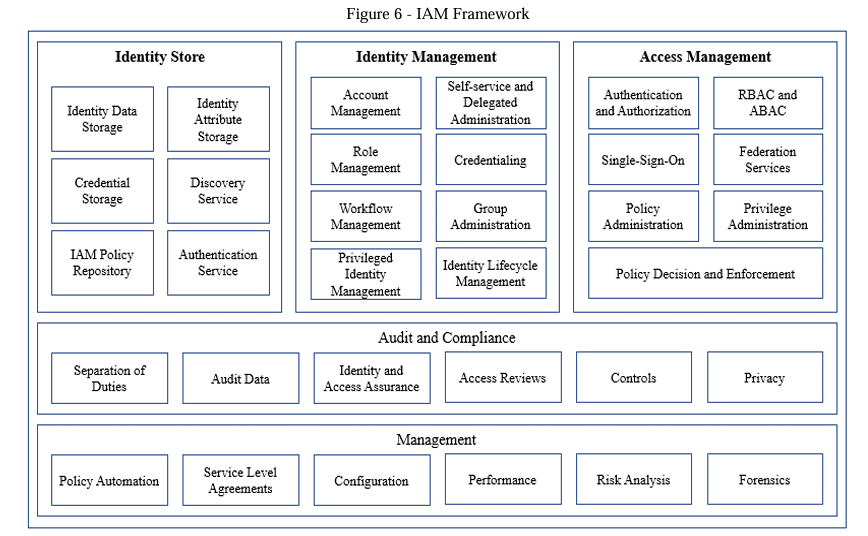
**What is IAM?**

“IAM stands for **Identity and Access Management**. It is a framework of policies and technologies for ensuring that the right individuals have the appropriate access to technology resources. IAM systems are used to initiate, capture, record, and manage user identities and their related access permissions. User Management, Authentication, Authorization, Access Management and Audit and Reporting are key components of IAM.”

**Why is there a need for IAM?**

1. **Security**: IAM helps protect sensitive information and resources by ensuring that only authorized individuals can access them. It reduces the risk of data breaches and cyber-attacks by implementing stringent authentication and authorization mechanisms.
2. **Compliance**: Organizations must comply with various regulations and standards (such as GDPR, HIPAA, and SOX) that mandate strict access controls and user identity management. IAM systems help organizations meet these regulatory requirements and avoid legal penalties..
3. **Scalability**: As organizations grow, managing identities and access rights manually becomes increasingly complex and error-prone. IAM systems offer scalable solutions that can accommodate the expanding user base and evolving access needs of a growing organization.
4. **Auditing and Accountability**: IAM provides detailed logs and reports on user activities, helping organizations monitor and audit access to critical systems and data. This transparency supports accountability and helps detect and respond to suspicious activities promptly.

Overall, IAM is essential for protecting organizational assets, ensuring regulatory compliance, enhancing operational efficiency, and delivering a positive user experience.



* 1. **Background Study**

1. The directory management tools that emerged in the 1990’s can be
2. seen as the start of the development of IAM systems (Rizvi, 2006), although that term was not introduced
3. until much later. Single Sign-on and Identity Administration followed, growing along with the number of
4. applications used in organizations.

7. 2
8. The current IAM market has its roots in a wide range of domains, as many of the different product areas
9. within the IAM market have started out as separate markets that flowed together over time (Cser, 2008).
10. However IAM is nowadays often considered to be a single market, the fragmented history of the field
11. explains why the IAM market still contains a variety of vendors, from pure players to companies that
12. offer comprehensive IAM solutions. A quote from the research vice president at Gartner describes the
13. situation within the current IAM market perfectly: “No company has bought tools from one vendor, or
14. implemented them all at once, They tend to solve their problems one at a time so most organizations are
15. somewhere along the automations track, but very few have done it all.” (Everett, 2007).
16. The directory management tools that emerged in the 1990’s can be
17. seen as the start of the development of IAM systems (Rizvi, 2006), although that term was not introduced
18. until much later. Single Sign-on and Identity Administration followed, growing along with the number of
19. applications used in organizations.

22. 2
23. The current IAM market has its roots in a wide range of domains, as many of the different product areas
24. within the IAM market have started out as separate markets that flowed together over time (Cser, 2008).
25. However IAM is nowadays often considered to be a single market, the fragmented history of the field
26. explains why the IAM market still contains a variety of vendors, from pure players to companies that
27. offer comprehensive IAM solutions. A quote from the research vice president at Gartner describes the
28. situation within the current IAM market perfectly: “No company has bought tools from one vendor, or
29. implemented them all at once, They tend to solve their problems one at a time so most organizations are
30. somewhere along the automations track, but very few have done it all.” (Everett, 2007).
31. The directory management tools that emerged in the 1990’s can be
32. seen as the start of the development of IAM systems (Rizvi, 2006), although that term was not introduced
33. until much later. Single Sign-on and Identity Administration followed, growing along with the number of
34. applications used in organizations.

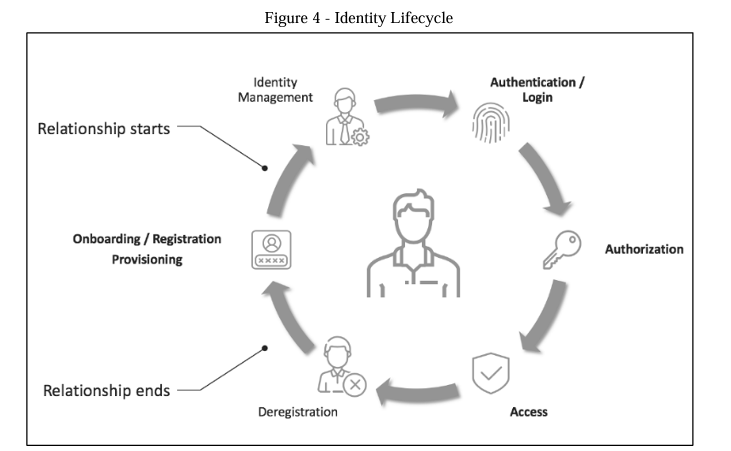
37. 2
38. The current IAM market has its roots in a wide range of domains, as many of the different product areas
39. within the IAM market have started out as separate markets that flowed together over time (Cser, 2008).
40. However IAM is nowadays often considered to be a single market, the fragmented history of the field
41. explains why the IAM market still contains a variety of vendors, from pure players to companies that
42. offer comprehensive IAM solutions. A quote from the research vice president at Gartner describes the
43. situation within the current IAM market perfectly: “No company has bought tools from one vendor, or
44. implemented them all at once, They tend to solve their problems one at a time so most organizations are
45. somewhere along the automations track, but very few have done it all.” (Everett, 2007).
46. The directory management tools that emerged in the 1990’s can be
47. seen as the start of the development of IAM systems (Rizvi, 2006), although that term was not introduced
48. until much later. Single Sign-on and Identity Administration followed, growing along with the number of
49. applications used in organizations.

52. 2
53. The current IAM market has its roots in a wide range of domains, as many of the different product areas
54. within the IAM market have started out as separate markets that flowed together over time (Cser, 2008).
55. However IAM is nowadays often considered to be a single market, the fragmented history of the field
56. explains why the IAM market still contains a variety of vendors, from pure players to companies that
57. offer comprehensive IAM solutions. A quote from the research vice president at Gartner describes the
58. situation within the current IAM market perfectly: “No company has bought tools from one vendor, or
59. implemented them all at once, They tend to solve their problems one at a time so most organizations are
60. somewhere along the automations track, but very few have done it all.” (Everett, 2007).
61. The directory management tools that emerged in the 1990’s can be
62. seen as the start of the development of IAM systems (Rizvi, 2006), although that term was not introduced
63. until much later. Single Sign-on and Identity Administration followed, growing along with the number of
64. applications used in organizations.

67. 2
68. The current IAM market has its roots in a wide range of domains, as many of the different product areas
69. within the IAM market have started out as separate markets that flowed together over time (Cser, 2008).
70. However IAM is nowadays often considered to be a single market, the fragmented history of the field
71. explains why the IAM market still contains a variety of vendors, from pure players to companies that
72. offer comprehensive IAM solutions. A quote from the research vice president at Gartner describes the
73. situation within the current IAM market perfectly: “No company has bought tools from one vendor, or
74. implemented them all at once, They tend to solve their problems one at a time so most organizations are
75. somewhere along the automations track, but very few have done it all.” (Everett, 2007)
76. The directory management tools that emerged in the 1990’s can be
77. seen as the start of the development of IAM systems (Rizvi, 2006), although that term was not introduced
78. until much later. Single Sign-on and Identity Administration followed, growing along with the number of
79. applications used in organizations.

82. 2
83. The current IAM market has its roots in a wide range of domains, as many of the different product areas
84. within the IAM market have started out as separate markets that flowed together over time (Cser, 2008).
85. However IAM is nowadays often considered to be a single market, the fragmented history of the field
86. explains why the IAM market still contains a variety of vendors, from pure players to companies that
87. offer comprehensive IAM solutions. A quote from the research vice president at Gartner describes the
88. situation within the current IAM market perfectly: “No company has bought tools from one vendor, or
89. implemented them all at once, They tend to solve their problems one at a time so most organizations are
90. somewhere along the automations track, but very few have done it all.” (Everett, 2007).

⮚ The digital identity lifecycle in Figure 4 represents each stage of identity within an organization. It describes the phases in which an identity goes through in an organization. First, the on boarding process takes place. From here onwards, the relationship starts then an integrated identity management platform handles the administration of the identity. An on boarding process involves the creation of digital identity. It is usually carried out by HR and within the human resource management system (HRMS). Provisioning is all about providing the digital identity appropriate access to the resource. It involves provisioning and designs-provisioning resources to entities. Based on the business role and privileges, the authentication mechanism is configured for that identity, which also involves giving authorization and access to the right resources based on the principles of least privileges. Once the lifespan of the identity is served, the human resource management system initiates a deregistration process. The digital identities are managed using an identity lifecycle management process defined in companies' IAM policy.



## AWS IAM — Key Features

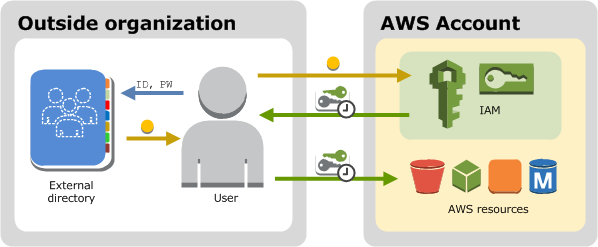
We should think of IAM as the first step towards securing all your AWS services and resources. Let’s look at some of the key features that make IAM so versatile and powerful:

* **Authentication:**AWS IAM lets you create and manage identities such as users, groups, and roles, meaning you can issue and enable authentication for resources, people, services, and apps within your AWS account. In the next section, we’ll look at authentication in detail.
* **Authorization:**Access management or authorization in IAM is made of two primary components: **Policies** and **Permissions**. In the next section, we’ll also look at each of these.
* **Fine-grained permissions:**Consider this — you want to provide the sales team in your organization access to billing information, but also need to allow the developer team full access to the EC2 service, and the marketing team access to selected S3 buckets. Using IAM, you can configure and tune these permissions as per the needs of your users.
* **Shared access to AWS accounts:**Most organizations have more than one AWS account, and at times need to delegate access between them. IAM lets you do this without sharing your credentials, and more recently, AWS released [ControlTower](https://aws.amazon.com/controltower/) to further simplify multi-account configurations. We also published a quick, hands-on tutorial on[Securing Multi-Account Access on AWS](https://blog.runpanther.io/secure-multi-account-aws-access/).
* **AWS Organizations:**For fine-grained control for multiple AWS accounts, you can use [AWS Organizations](https://aws.amazon.com/organizations/) to segment accounts into groups and assign permission boundaries.
* **Identity Federation:**Many times, your organization will need to federate access from other identity providers such as Okta, G Suite, or Active Directory. IAM enables you to do this with a feature called [Identity Federation](https://aws.amazon.com/about-aws/whats-new/2011/08/03/Announcing-IAM-Identity-Federation/).

# Authentication in IAM

Authentication or identity management in AWS IAM consists of the following identities:

1. **Users:**An IAM user is a person that needs to interact with your AWS resources or services either from the AWS Console or with the AWS CLI. When you create a new user, no credentials are assigned, and the user does not have any permission to access your AWS resources.
2. **Groups:**An IAM group is a collection of users and permissions assigned to those users. Groups provide a convenient way to manage permissions for users with similar needs by categorizing them according to their job function/role, department, or any other requirement. Then, permissions for all those users can be managed at once through the group.
3. **Roles:**An IAM role is an entity within AWS which defines a set of permissions the role can perform, and what entities can assume the role. A role is not directly linked to a person or a service, rather it can be assumed by any resource that the role grants permission to. Role credentials are always temporary and rotated periodically by the AWS Session Token Service (STS). For this reason, it is recommended to use roles over directly granting user or group permissions. Additionally, Roles allow you to grant multi-account access to your AWS resources from users, services, and apps that aren’t part of your business. The concepts of users and groups will be familiar to most system administrators, but IAM Roles can often be unfamiliar. Let’s dive into more details below.



IAM roles fulfill a unique and powerful niche in the identity and access management landscape. Instead of assigning permissions to an entity directly, roles allow an entity to be granted permissions temporarily (on an as-needed basis) to perform tasks. This enforces the least privilege principle which is based on both identity and time, as you can restrict entities to both the minimum amount of access needed as well as the minimum amount of time needed to complete a task.

Consider this: an administrator in your organization accidentally issues a command to delete a production resource. In an environment where permissions are controlled entirely with users and groups, this command would go through. On the contrary, in an environment controlled with roles, this command would only go through if the administrator had recently assumed the **DeleteProductionResources** role, or something similar. This allows services and users to have the capability to do everything their tasks require while minimizing the risk of compromised credentials and systems.

# Authorization in IAM

Authorization or access management in IAM is controlled by **Policies** that grant **Permissions**.

## What is a Policy?

A policy is a document with a set of rules, having one or more statements. Each policy grants a specific set of permissions and can be attached to any of the IAM identities we covered earlier — users, groups, and roles. Policies are always written in JSON or YAML format and each policy has a name.

There are two types of policies you should know about:

1. **Managed policies:**Managed policies can be created and attached to multiple entities. AWS has built-in managed policies that cover a wide variety of use cases. Managed policies can also be mixed and matched to provide generalized access to roles, users, or groups. AWS customers can also create their own managed policies.
2. **Inline policies:**These policies are directly applied to IAM entities, and do not have distinctive ARNs. You use inline policies for a specific objective, which makes them non-reusable.

AWS recommends the use of managed policies instead of inline policies so that permissions are more standardized and can be reused.

## What are Permissions?

Permissions enable you to perform actions on AWS resources. When a new user or group is created, it has no permissions and a policy must be attached to allow actions to be taken on AWS resources.

You can assign permissions to all AWS identities (users, groups, and roles). Permissions are assigned in the following two ways:

* **Identity-based**: Policies attached directly to users, groups, or roles
* **Resource-based**: Policies attached to AWS resources, such as S3 Buckets, ECR Repositories, and more

When writing new policies, the following resources can be helpful:

* [Manage IAM Permissions](https://aws.amazon.com/iam/features/manage-permissions/): This page offers quick reference to help you assign and manage IAM permission
* [Actions, Resources, and Condition Keys](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_actions-resources-contextkeys.html): A comprehensive reference to all possible actions that can be taken on various AWS services
* [AWS Policy Simulator](https://policysim.aws.amazon.com/home/index.jsp?): Validate that newly created policies work end-to-end by creating access simulations

Generally, policies should follow the principle of least privilege, which means only the absolute minimum set of access should be granted to get the job done. Policies can be extremely specific — consider the following code block, for example:

{  
 "Version": "2012-10-17",  
 "Statement": [  
 {  
 "Action": [  
 "iam:ChangePassword",  
 "iam:CreateLoginProfile",  
 "iam:DeleteLoginProfile",  
 "iam:GetLoginProfile",  
 "iam:GetUser",  
 "iam:UpdateLoginProfile"  
 ],  
 "Resource": "arn:aws:iam::\*:user\/${aws:username}",  
 "Effect": "Allow",  
 "Sid": "AllowManageOwnPasswords"  
 }  
 ]  
}

Or policies can be broadly defined, such as in the following code block:

{  
 "Version": "2012-10-17",  
 "Statement": [  
 {  
 "Action": [  
 "iam:\*"  
 ],  
 "Resource": "\*",  
 "Effect": "Allow",  
 "Sid": "IAMAdmin"  
 }  
 ]  
}

Finding the right balance is important, as overly granular policies lead to undue overhead, and overly broad policies can lead to inappropriate access, which is a major factor in security breaches. Following the principle of least privilege can go a long way in ensuring that only a minimal amount of damage occurs during unexpected security events.

**CONCLUSION**

Identity and Access Management (IAM) is an indispensable component of modern organizational security and operational strategy. Its role in safeguarding sensitive data, ensuring regulatory compliance, and enhancing user experience cannot be overstated. By implementing a robust IAM framework, organizations can mitigate security risks, streamline administrative processes, and support scalable growth. IAM not only fortifies the digital defenses of an organization but also promotes efficiency and accountability through precise access controls and comprehensive auditing. As the digital landscape continues to evolve, the importance of a well-designed IAM system becomes even more critical, making it a foundational element for any forward-thinking organization committed to maintaining security, compliance, and operational excellence.

**References :**Active Directory Domain Services on AWS. (2018). Amazon Web Services: https://d1.awsstatic.com/whitepapers/adds-on-aws.pdf Ahmed K.E.U., A.V. (2011). Identity and Access Management in Cloud Computing. Cloud Computing for Enterprise Architectures. Computer Communications and Networks. Springer. Amazon Web Services. (2018). Active Directory Domain Services on AWS. Retrieved from https://d1.awsstatic.com/whitepapers/adds-on-aws.pdf Baldwin, A., Casassa Mont, M., Beres, Y., & Shiu, S. (2010). Assurance for Federated Identity Management. Journal of Computer Security, 519–550. Columbus, L. (2019). 74% Of Data Breaches Start With Privileged Credential Abuse. Forbes: https://www.forbes.com/sites/louiscolumbus/2019/02/26/74-of-data-breaches-start-with-privileged credential-abuse/#114c3fd73ce4 E. Bertino, K. T. (2011). Identity Management: Concepts, Technologies, and Systems. Artech House. F. Damon and M. Coetzee. (2013). Towards a generic Identity and Access Assurance model by component analysis - A conceptual review. Proceedings of the First International Conference on Enterprise Systems. Cape Town.