IAM Architecture

Y. V. Lokeswari
AP / CSE
SSN College of Engineering

Identity & Access Management

- Security in any system involves primarily ensuring that the **right entity** gets **access** to only the **authorized data** in the **authorized format** at an **authorized time** and from an **authorized location**.
- Identities, trust, authentication and access controls have obtained additional significance in the cloud world.
- **Identity and access management (IAM)** is of prime importance in this regard.
- Identity and Access Management (IAM) is used to manage **access** to **resources** by assuring that the **identity** of an **entity** is **verified**, then **granting** the **correct level** of **access** based on the **protected resource**.

Identity & Access Management

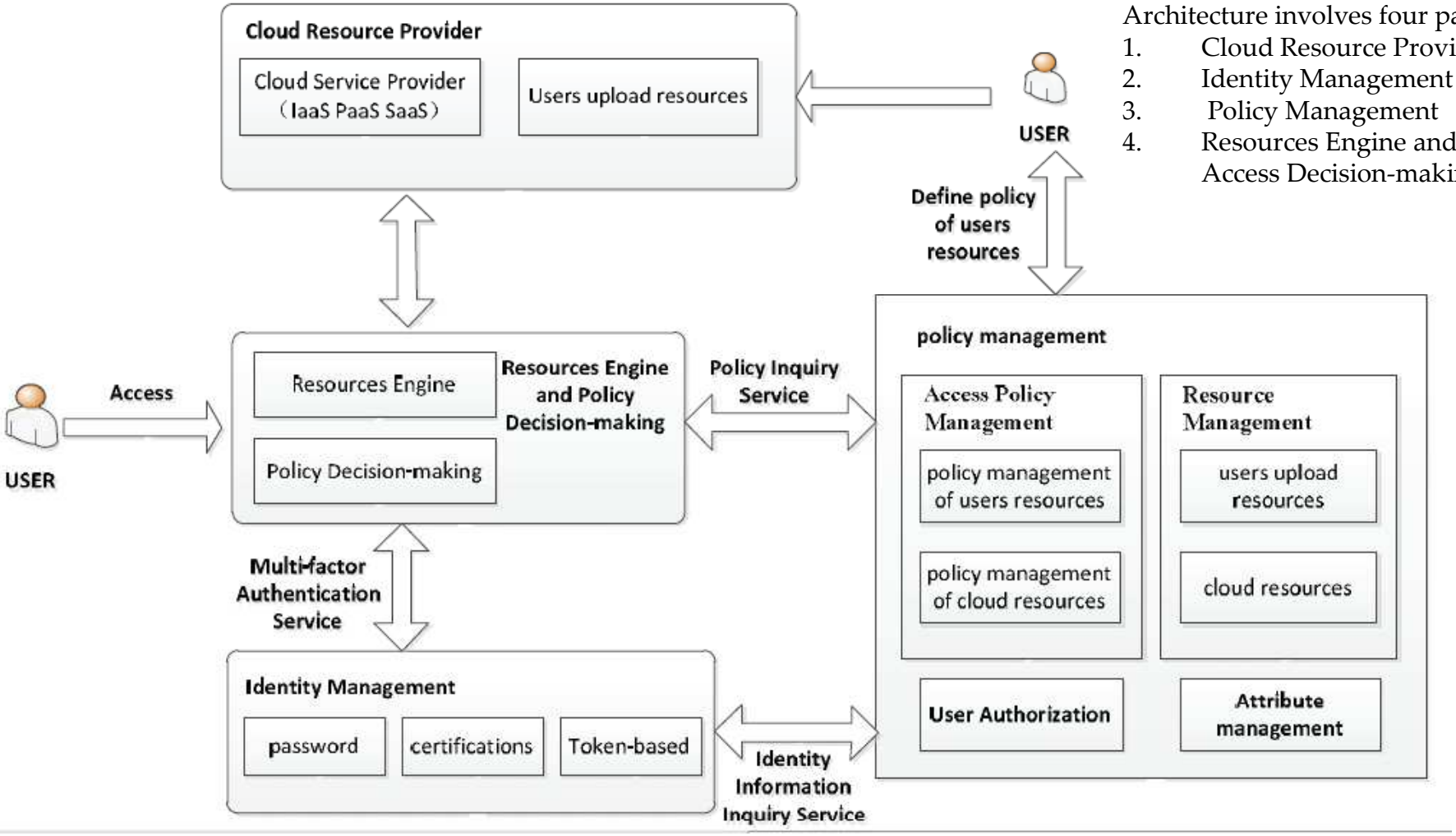
- Identity and access management is a critical function for every organization, and a fundamental expectation of SaaS customers

  The principle of least privilege states
- "*Only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary*".
- The advent of cloud services and services on demand is changing the identity management landscape.
- Most of the current identity management solutions are focused on the enterprise and typically are architected to work in a very controlled in static environment

Identity & Access Management

- Main Functions of IAM
  - **Identity Provisioning**
  - **Authentication**
  - **Authorization**
  - **Policy Management**

Identity & Access Management Architecture



Architecture involves four parts

1. Cloud Resource Provider
2. Identity Management
3. Policy Management
4. Resources Engine and Access Decision-making.

Identity & Access Management Architecture

1. **Cloud Resource Provider (CRP)** : The resource provider is responsible for providing access to resources based on user's asserted identity and privilege.

•**Cloud resources** : involve software, operating systems or even programming environment and network infrastructure.

•**User upload resources** are mainly user-generated resources and upload their own resources to the cloud, which provide the data access to the users.

Identity & Access Management Architecture

2. Identity Management (IDM) : IDM is responsible for managing users and their identities, issuing credentials, vouching for the user's identity and identity assertion.
It provides two external services:

- **Multi-factor Authentication Service**: is the interface provided by IDM to validates the asserted identity information.
    - The authentication services evaluate credentials such as user name and password, secure ID token pass phrases, X.509 certifications, and so on, directly provided by the user.
- **Identity Information Inquiry Service**: is the interface provided by IDM to check the identity information for user authorization.

Identity & Access Management Architecture

3. Policy Management (PM): Policy management enforces access rules that associate users with resources.

Policy management supports 5 functions:

1. Attribute Management
2. User authorization
3. Resource management
4. Access policy management : Access Policy Management defines access rules of cloud resources and users own resources.
5. Policy Inquiry Service : Policy Inquiry Service is available to query the user privileges and according to resource access policies, decide whether to allow users to access

Identity & Access Management Architecture

4. Resources Engine and Policy Decision-making(REPD) :

- **Resources Engine (RE):** Resources Engine implements scheduling of resources within cloud. This component is responsible for finding resources that meets the requirements of the user among the list of resource.

- **Policy Decision-making (PD):** Policy Decision-making determines whether to allow users to access appropriate resources by assuring security. It takes the help of IDM and Policy Management component.

References

- Yang, Yan, Xingyuan Chen, Guangxia Wang, and Lifeng Cao. "An Identity and Access Management Architecture in Cloud." In *Computational Intelligence and Design (ISCID), 2014 Seventh International Symposium on*, vol. 2, pp. 200-203. IEEE, 2014.