IAM Practices in Cloud

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

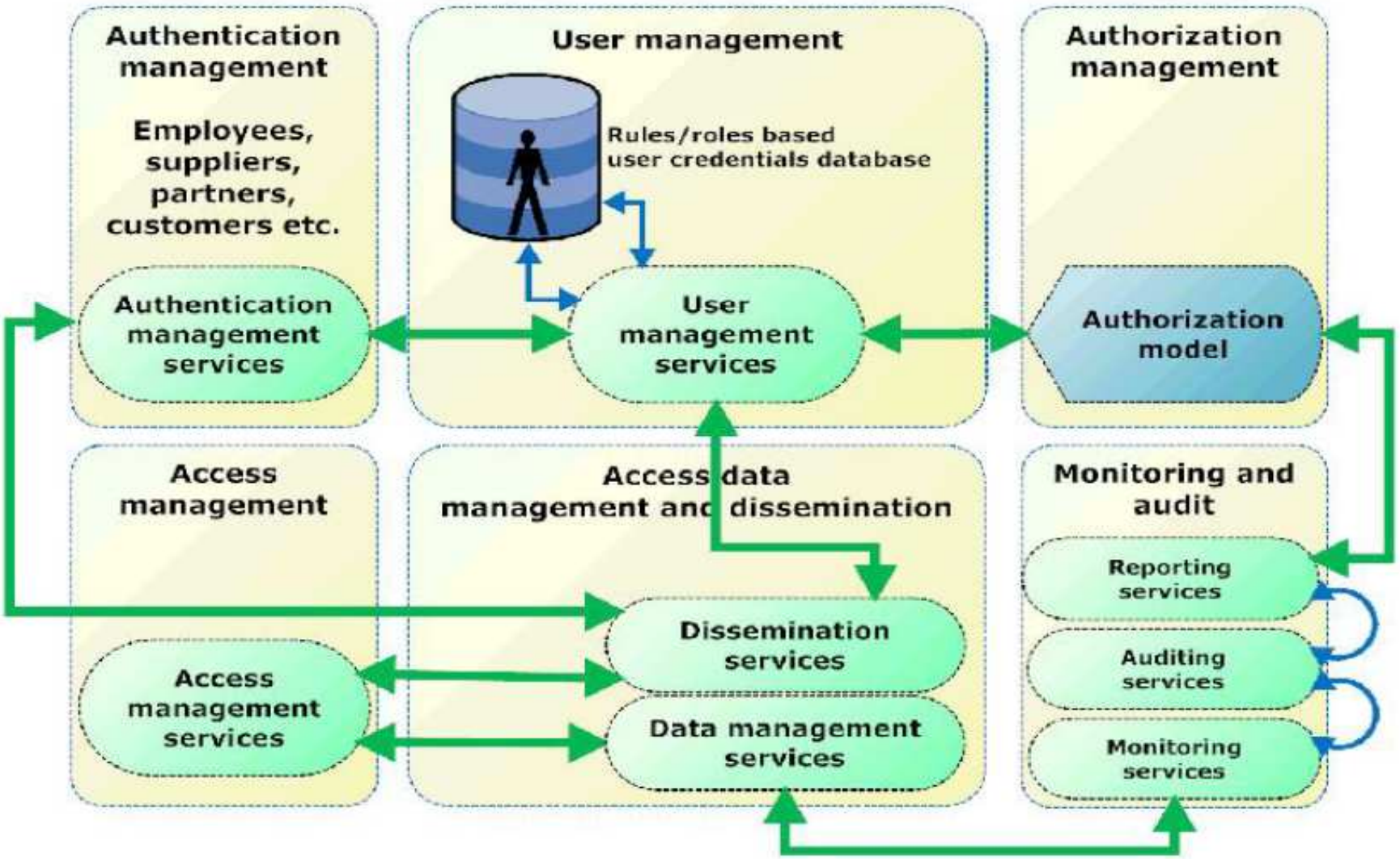
Identity & Access Management Practices

- Core Process
  - **User management**
  - **Authentication management**
  - **Authorization management**
  - **Access management**
  - **Management and dissemination of access data**
  - **Audit and operational monitoring**

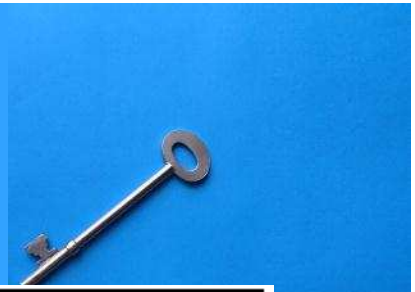
Identity & Access Management Practices

- IAM Activities
  - **Attributes management**
  - **Authorization policies management**
  - **External identities management**
  - **Compliance management**
  - **Authentication and authorization centralization**

IAM Functional Architecture

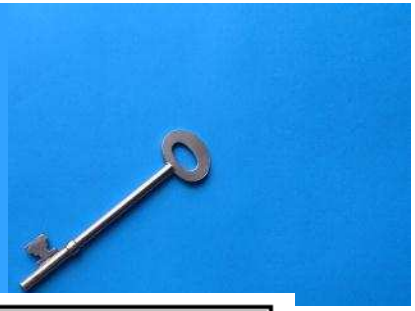


Identity & Access Management Standards



Standard or protocol name	Supporting companies	Open standard	Cloud provider requests	Cloud beneficiary requests
SAML	Oracle, IBM, Novell, Computer Associates, Microsoft, Sympified, TriCipher, Ping Identity	YES	Allow customers to delegate authentication and choose authentication methods that enable adoption of the cloud service.	Strong authentications, Web-based SSO, avoid identity duplication; protect privacy by sharing attributes only by consent.
XACML	Oracle, Computer Associates, Jericho Systems, IBM, CISCO, Securent, Red Hat	YES	Allow authorization that may represent complex policies, required by enterprise-scale applications and administrators.	A standardized mean to formulate authorization policies across a large set of cloud services and separate authorization and enforcement procedures from the application.

Identity & Access Management Standards



Standard or protocol name	Supporting companies	Open standard	Cloud provider requests	Cloud beneficiary requests
OAuth	Google, Twitter, Facebook, Plaxo	YES	Allow users to access their data (hosted by another service provider) while protecting their account and credentials information, which is not sent.	Publish and interact with protected data stored by one provider and accessed by another provider using a standard API and without disclosing credentials.
OpenID	Google, IBM, Microsoft, yahoo, Orange, payPal, VeriSign, AOL, Yandex, UStream	YES	Provides SSO for consumers participating in this federated identity service.	Adoption avoided due to some trust issues.
OATH	VeriSign, SanDisk, Gemalto, Entrust	YES	Unification across three widely used industrial standards.	Unification across three widely used industrial standards.
OpenAuth	AOL and partners	NO	Support AOL users access to third party applications using AOL or AIM user IDs.	Support for single authentication across multiple applications (by AOL partners only).

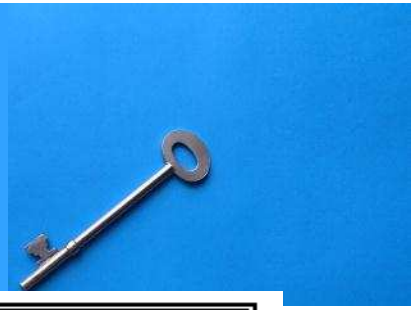
Identity & Access Management in Cloud

- The methods of access and **identity management** used directly in the cloud are still in an **early development stage**.
- The **standards of security management** in the cloud are extremely **diverse**, **differing** significantly from **one provider** to another, regardless of the provided cloud computing component (software, platform or infrastructure).

Table 2. **Cloud-based *IAM* maturity levels**

DOMAIN	SAAS	PAAS	IAAS
User Management, New Users	Capable	Immature	Aware
User Management, User Modifications	Capable	Immature	Immature
Authentication Management	Capable	Aware	Capable
Authorization Management	Aware	Immature	Immature

IAM Approaches Comparison



	Organization-based identity services provider	Cloud-based identity services provider
Strong points	• Consistent with internal policies, processes and access management • Direct access to the service-level agreement and the identity provider's security level • Incremental investment in the existing identity architecture in order to assure federation in the future	• Some cloud identity management use cases are migrated to the cloud-based services provider, hiding the complexity of some standards (or versions of the standards) • Only small architectural changes are needed • Once the synchronization is complete, users can sign to cloud applications using corporate credentials and authentication policies
Weak points	• In the absence of federation, the addition of the identity life cycle management for non-employees may lead to serious inefficiencies	• Lack of details visibility, as the company relies on a third party • Overall performance depends solely on the performance level of the cloud service provider, not fully visible for the beneficiary • The lack of detailed reports for compliance reporting • Non-uniform attribute definition may render the process very complex (complex synchronization)

References

- Mangiuc, Dragos Marian. "Cloud Identity and Access Management-A Model Proposal." *Accounting and Management Information Systems* 11, no. 3 (2012): 484.