Data Security and Storage

- Several aspects of data security, including:
- Data-in-transit
- Data-at-rest
- Processing of data, including multitenancy
- Data lineage
- Data provenance
- Data remanence

Aspects of Data Security

- **Data-in-transit**-
  - encryption algorithm.
  - Secure protocol like https(not http)
- **Data-at-rest –**
  - Iaas.
  - For paas- saas?
- **Processing of data, including multitenancy**
  - What if data is to be processed at cloud?
  - IBM

- **Data lineage**
  - audit or compliance purposes
  - Following the path of data
- **Provenance**
  - computationally accurate
- **Data remanence**
  - Residue
  - inadvertent disclosure of sensitive information

Data Security Mitigation

- to ensure that any sensitive or regulated data is not put into a public cloud.
- Provider Data and Its Security-What data your CSP collects and how it monitors and protects that data is important to the provider for its own audit purposes
- Storage-confidentiality, integrity, and availability

Confidentiality

- access control
  - Authentication –generally weak(username+password)
  - Authorization-csp less levels-admins and users
- Protection of the stored data
  - Encryption algorithm- is there any? If yes,key strength?
  - S3 doesn’t encrypt.
  - If encrypts-type of encryption, key length, key management

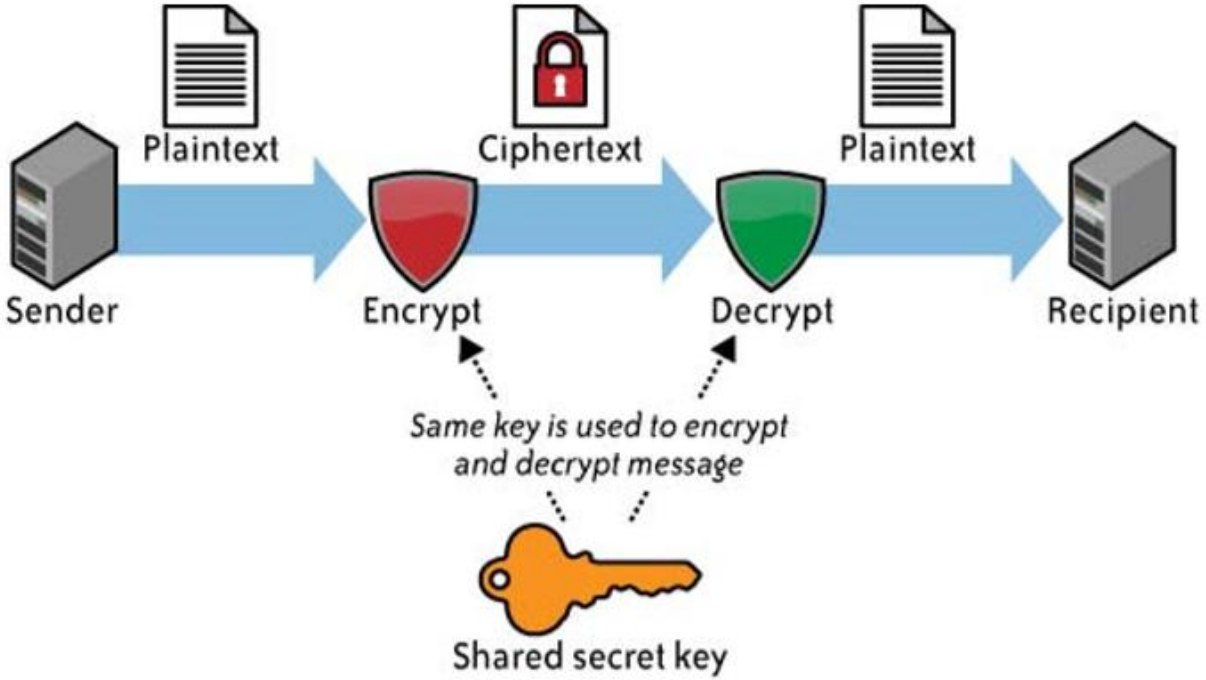

FIGURE 4-1. Symmetric encryption

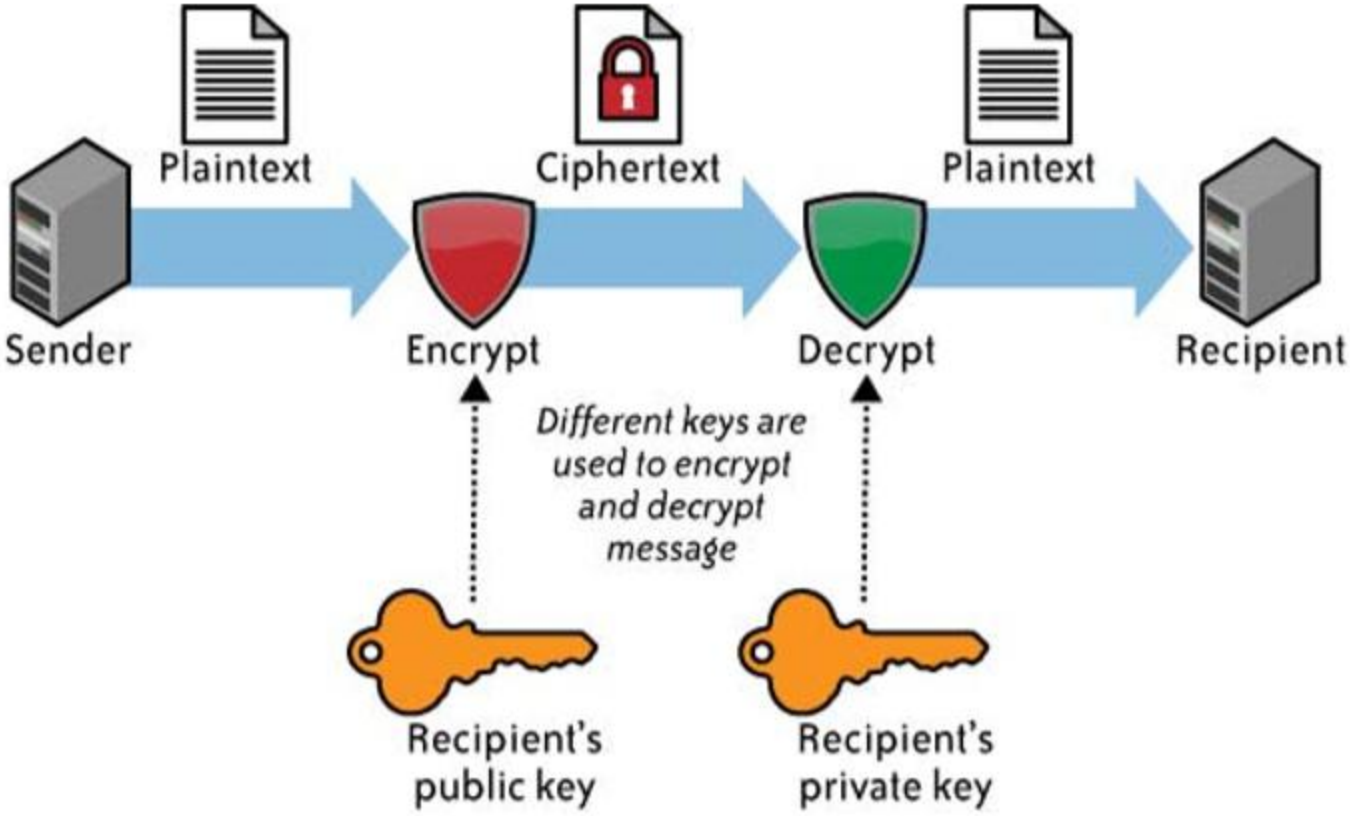

FIGURE 4-2. Asymmetric encryption

It would be highly unusual to use an asymmetric algorithm for encryption of the LARGE VOLUME because of the speed and computational efficiency issues.

Integrity

- In addition to the confidentiality of your data, you also need to worry about the integrity of your data.
- Message authentication codes (MACs)
- customer has several gigabytes (or more) of its data up in the cloud for storage, how does the customer check on the integrity of the data stored there?
- There are IaaS transfer costs associated with moving data into and back down from the cloud, as well as network utilization (bandwidth) considerations for the customer's own network.
- Even more difficult- without explicit knowledge of the whole data set-which physical machines their data is stored, or where those systems are located-probably dynamic and changing frequently.
- Those frequent changes obviate the effectiveness of traditional integrity insurance techniques.

Availibility

- threat to availability is network-based attacks- discussed in infrastructure security
- CSP's own availability-99.999%
- Actual loss
- CSP business shutdown
- stored data is actually backed up

Identity and Access Management

Trust Boundaries and IAM

- In a typical organization where applications are deployed within the **organization's perimeter** the "trust boundary" is **mostly static** and is monitored **and controlled by the IT department**.
- In that traditional model, the trust boundary encompasses the **network, systems, and applications hosted in a private data center** managed by the IT department (sometimes third-party providers under IT supervision).
- And **access** to the network, systems, and applications is secured via network security controls including **virtual private networks (VPNs), intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and multifactor authentication.**

After adoption of cloud…

- With the adoption of cloud services, the organization's trust boundary will become **dynamic** and will move **beyond the control of IT**.
- With cloud computing, the network, system, and application boundary of an organization will extend into **the service provider domain.**
- To **compensate** for **the loss** of network control and to strengthen risk assurance, **organizations will be forced** to rely on other **higher-level software controls**, such as **application security** and **user access controls.**

- These controls manifest as strong **authentication**, **authorization based on role or claims**, trusted sources with accurate attributes, **identity federation, single sign-on (SSO), user activity monitoring, and auditing**.
- **Federated identity** allows authorized users to access **multiple applications and domains using a single set of credentials**. It links a user's identity across multiple identity management systems so they can access different applications securely and efficiently.
- Federation coupled with good IAM practice can enable strong authentication by way of delegation, **web single sign-on**, and **entitlement management via centralized access control services**, it will play a central role in accelerating cloud computing adoption within organizations.

- One example of federated identity is when a user logs into a third-party website by using their **Gmail login** credentials.
- With FIM, they don’t have to create new credentials to access multiple websites that have a **federated agreement with Google**, such as:
- YouTube
- Fitbit
- Waze
- Picasa
- Blogger

Similarly, a user can use **their Facebook** credentials to log into many websites that are federated with Facebook, like:

- Instagram
- Netflix
- Disney+

Federated Identity vs Single Sign-on

- FIM and Single Sign-on (SSO) enable organizations to minimize password-related risks and secure their data and improve user experiences.
- Both kinds of solutions require a single set of credentials to grant the user access to multiple applications. But despite this similarity, these systems operate differently.
- With SSO, users can access multiple applications within the same organization or domain using a single set of credentials.
- Federated identity goes a step further. It enables users to access applications or platforms across multiple enterprise domains that are part of the federated configuration.
- Thus, FIM supports SSO and also extends SSO to multiple domains. Also, SSO is a function of FIM, but implementing it doesn’t necessarily allow for FIM.

- In some cases, the practice of IAM within an organization may suffer due to a **lack of central governance and identity information architecture**.
- More often than not, identity storage is managed **via manual entry** by **multiple administrators**, and user provisioning processes are not well orchestrated.
- This process is **inefficient.**
- In such cases, **the weak access model** will extend excess privileges for unauthorized users to cloud services

- CSPs **need to support IAM standards** (e.g., SAML) and **practices such as federation for customers** to take advantage of and extend their practice to maintain compliance with internal policies and standards.
- Cloud services that support IAM features such as federation will **accelerate the migration of traditional IT applications** from trusted corporate networks into a trusted cloud service model.
- For **customers**, well-implemented user IAM practices and processes will help protect the **confidentiality and integrity** and manage compliance of the information stored in the cloud.

Why IAM?

- Improve operational efficiency
- Properly architected IAM technology and processes can improve efficiency by automating user on-boarding and other repetitive tasks (e.g., self-service for users requesting password resets that otherwise will require the intervention of system administrators using a help desk ticketing system).
- Regulatory compliance management
- To protect systems, applications, and information from internal and external threats (e.g., disgruntled employees deleting sensitive files) and to comply with various regulatory, privacy, and data protection requirements, organizations implement an "IT general and application-level controls" framework derived from industry standard frameworks such as ISO 27002 and Information Technology Infrastructure Library (ITIL).
- IAM processes and practices can help organizations meet objectives in the area of access control and operational security (e.g., enforcement of compliance requirements such as "segregation of duties" and assignment of limited privileges for staff members to perform their duties).

Cloud use cases that require IAM support from the CSP include…

- **Employees** and on-site contractors of an organization accessing a SaaS service using identity federation (e.g., **sales and support** staff members accessing Salesforce.com with corporate identities and credentials)
- **IT administrators** accessing the CSP management console to provision resources and access for users using a corporate identity (e.g., IT administrators of Newco.com provisioning virtual machines or VMs in Amazon's EC2 service, configured with identities, entitlements, and credentials for operating the VMs [i.e., start, stop, suspend, and delete VMs])
- **An application** residing in a cloud service provider (e.g., Amazon EC2) accessing storage from another cloud service (e.g., Mosso).
- etc

IAM Challenges

- One critical challenge of IAM concerns **managing access for diverse user populations** (employees, contractors, partners, etc.)
- IT is constantly challenged to rapidly provision appropriate access to the users **whose roles and responsibilities often change for business reasons.**
- Access policies for information are **seldom centrally and consistently** applied. **Complex webs of user identities, access rights, and procedure**s led to inefficiencies in user and access management processes while exposing these organizations to **significant** security, regulatory compliance, and reputation **risks.**
- To address these challenges and risks, many companies have sought technology solutions to enable centralized and automated user access management.

IAM Definitions

Authentication

- Authentication is the process of verifying the identity of a user or system.

Authorization

- Authorization is the process of determining the privileges the user or system is entitled to once the identity is established. In the context of digital services, authorization usually follows the authentication step and is used to determine whether the user or service has the necessary privileges to perform certain operations—in other words, authorization is the process of enforcing policies.

IAM Definitions

- Auditing
- In the context of IAM, auditing entails the process of review and examination of authentication, authorization records, and activities to determine the adequacy of IAM system controls, to verify compliance with established security policies and procedures (e.g., separation of duties), to detect breaches in security services (e.g., privilege escalation), and to recommend any changes that are indicated for countermeasures.

IAM Architecture and Practice

User management

- Activities for the effective governance and management of identity life cycles

Authentication management

- Activities for the effective governance and management of the process for determining that an entity is who or what it claims to be.

Authorization management

- Activities for the effective governance and management of the process for determining entitlement rights that decide what resources an entity is permitted to access in accordance with the organization’s policies

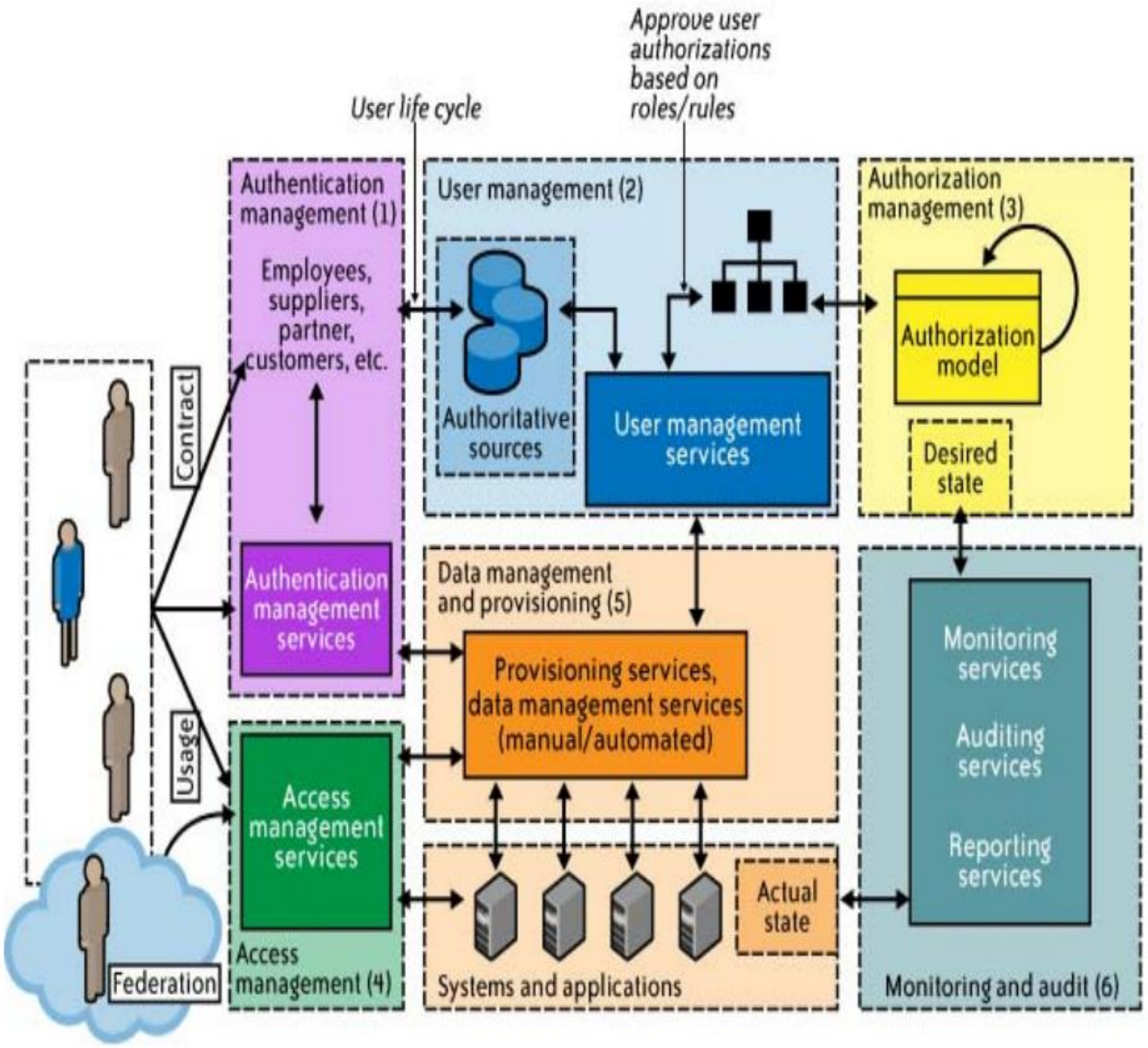

FIGURE 5-1. Enterprise IAM functional architecture

- Access management
- Enforcement of policies for access control in response to a request from an entity (user, services) wanting to access an IT resource within the organization

Data management and provisioning

- Propagation of identity and data for authorization to IT resources via automated or manual processes

Monitoring and auditing

- Monitoring, auditing, and reporting compliance by users regarding access to resources within the organization based on the defined policies

TRUST, REPUTATION, RISK

Trust

- “the willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trusting party, irrespective to the ability to monitor or control the trusted party”
- Trust is a subjective expectation an agent has about another‟s future behaviour that is based on the history of their encounters
- “Trust is the extent to which one party is willing to depend on something or some person in a given situation with a feeling of relative security, even though negative consequences are possible.”

Classification of trust

- Subjective trust vs. Objective trust
- Transaction-based vs. Opinion-based
- Complete information vs. Localized information
- Rank-based vs. Threshold-based

- Capability of an entity's trustworthiness being measured objectively against a universal standard, results in objective trust.
- If the trust being measured depends on an individual‘s tastes and interest, the resulting trust is called subjective trust.
- Decisions made based on the individual transactions and their results is known as transaction based trust, whereas the trust built based on just opinion of the individuals, is opinion based trust.
- If the trust building operation requires information from each and every node, it is called, complete information and it is known as either global trust function or complete trust function.
- If the information collected only from one‘s neighbors, it is called, localized information trust function.
- If the trust worthiness of an entity is ranked from the best to worst, it is rank based trust whereas the trust declared yes or no depending on preset trust threshold is known as threshold based trust.

Reputation

- When making trust-based decisions, entities can rely on others for information regarding to a specific entity.
- Reputation is public knowledge and represents the collective opinion of members of a group and it is based on the cumulative trust opinion of a group of agents.
- Definition of Reputation
- The reputation of an entity is an expectation of its behavior based on other entities' observations or information about the entity's past behavior within a specific context at a given time.

Basic Security Risk Considerations

- **Organizational Security Risks**
- Organizational risks are categorized are categorized as the risks that may impact the structure of the organization or the business as an entity.
- For example, if a CSP goes out of business or gets acquired by another entity, this may negatively affect their CSPs since any Service Level Agreements (SLA) they had may have changed and they would then have to migrate to another CSP that more closely aligns with their needs.

- **Physical Security Risks**
- The physical location of the cloud data center must be secured by the CSP in order to prevent unauthorized on-site access of CSC data. Even firewalls and encryption cannot protect against the physical theft of data. Since the CSP is in charge of the physical infrastructure, they should implement and operate appropriate infrastructure controls including staff training, physical location security, network firewalls. It is also important to note that the CSP is not only responsible for storing and process data in specific jurisdictions but is also responsible for obeying the privacy regulations of those jurisdictions.

- **Technological Security Risks**
- These risks are the failures associated with the hardware, technologies and services provided by the CSP. In the public cloud, with its multi tenancy features, these include resource sharing isolation problems, and risks related to changing CSPs, i.e. portability. Regular maintenance and audit of infrastructure by CSP is recommended.

- **Compliance and Audit Risks**
- These are risks related to the law. That is, risks related to lack of jurisdiction information, changes in jurisdiction, illegal clauses in the contract and ongoing legal disputes. For example, depending on location, some CSPs may be mandated by law to turn over sensitive information if demanded by government.

- **Data Security Risks**
- There are a variety of data security risks that we need to take into account. The three main properties that we need to ensure are data integrity, confidentiality and availability.

source

- https://journals-sathyabama.com/archives/acm/NAT-CSE-OCT-2015_Vol6-No2-1.pdf
- https://www.cse.wustl.edu/~jain/cse570-15/ftp/cld_sec/index.html
- https://arxiv.org/ftp/arxiv/papers/1211/1211.3979.pdf