SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107
Accredited by NAAC-UGC with 'A' Grade
Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

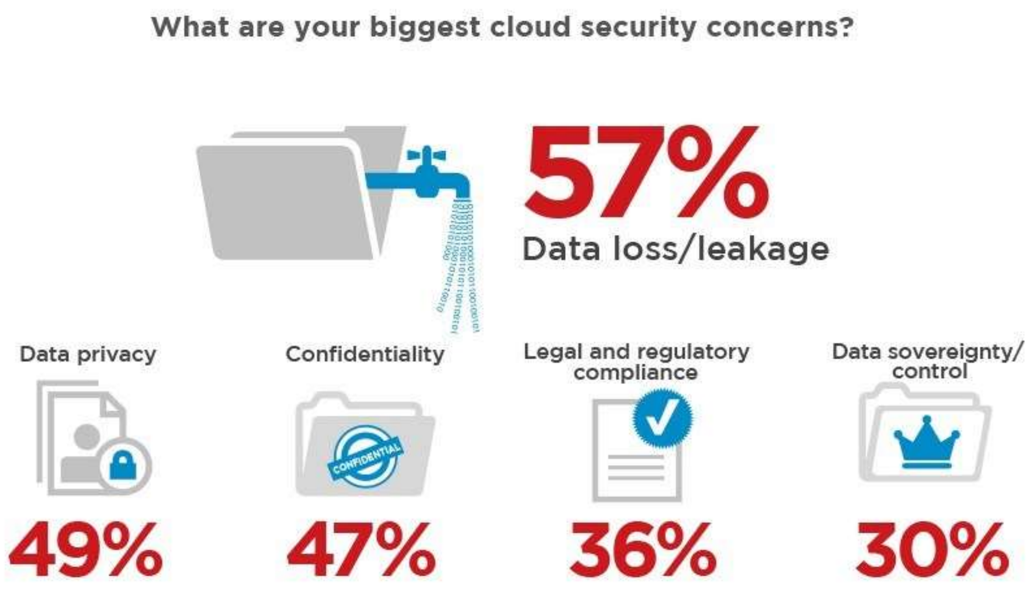
Department of Information Technology

Topic 5 – Security Challenges

Security Challenges

Lose of control of our own Data

- In the cloud, you lose control over assets in some respects, so your security model must be reassessed.
- Can you trust your data to your service provider?
- With the cloud model, you lose control over physical security.
- In a public cloud, you are sharing computing resources with other companies.
- In a shared pool outside the enterprise, you don't have any knowledge or control of where the resources run.



Security Challenges

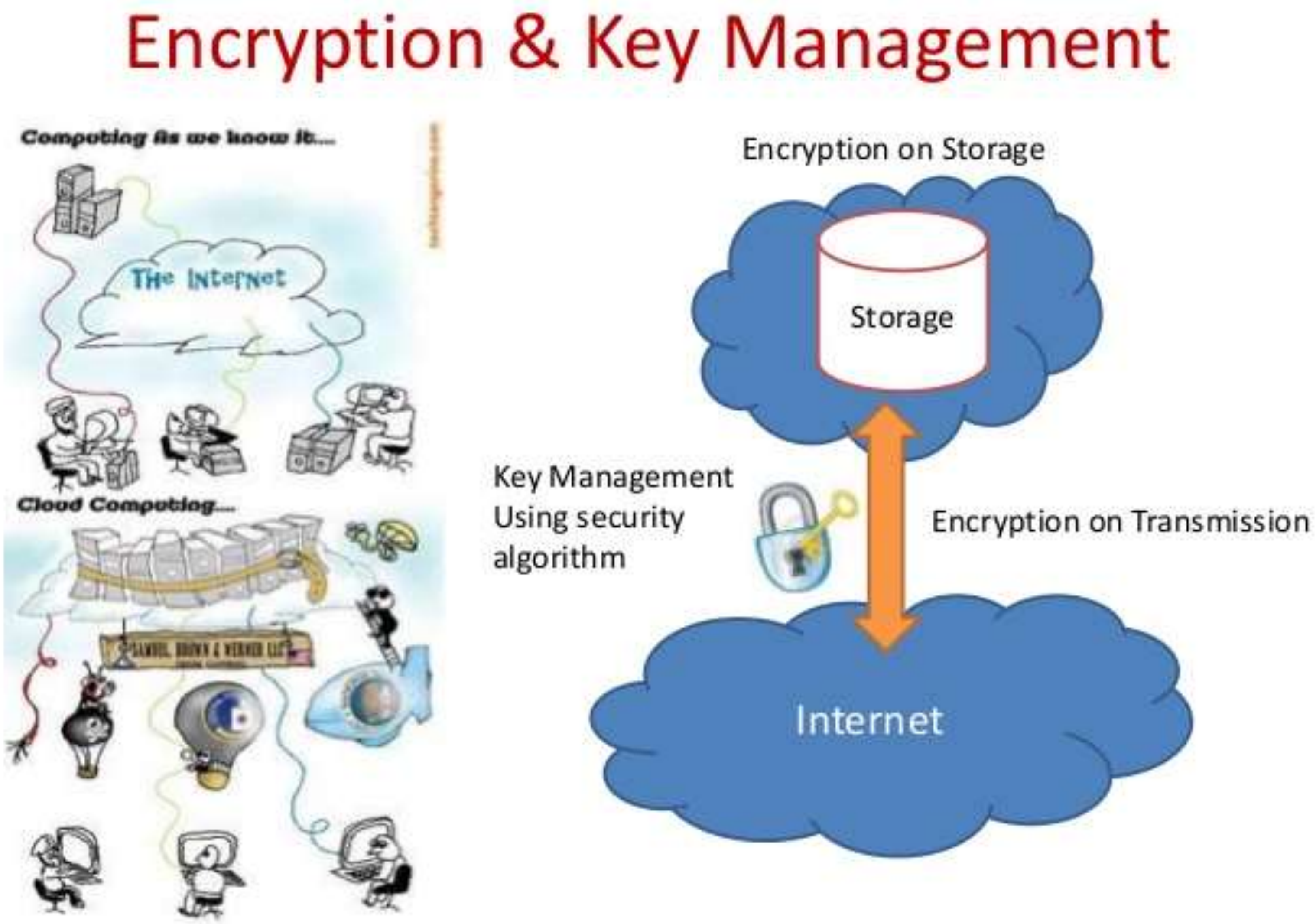
Encryption Standards

If information is encrypted while passing through the cloud, who controls the encryption/decryption keys? Customer or Vendor?

Most customers probably want their data encrypted both ways across the Internet using SSL (Secure Sockets Layer protocol)

They also most likely want their data encrypted while it is at rest in the cloud vendor’s storage pool.

Be sure that you, the customer, control the encryption/ decryption keys.



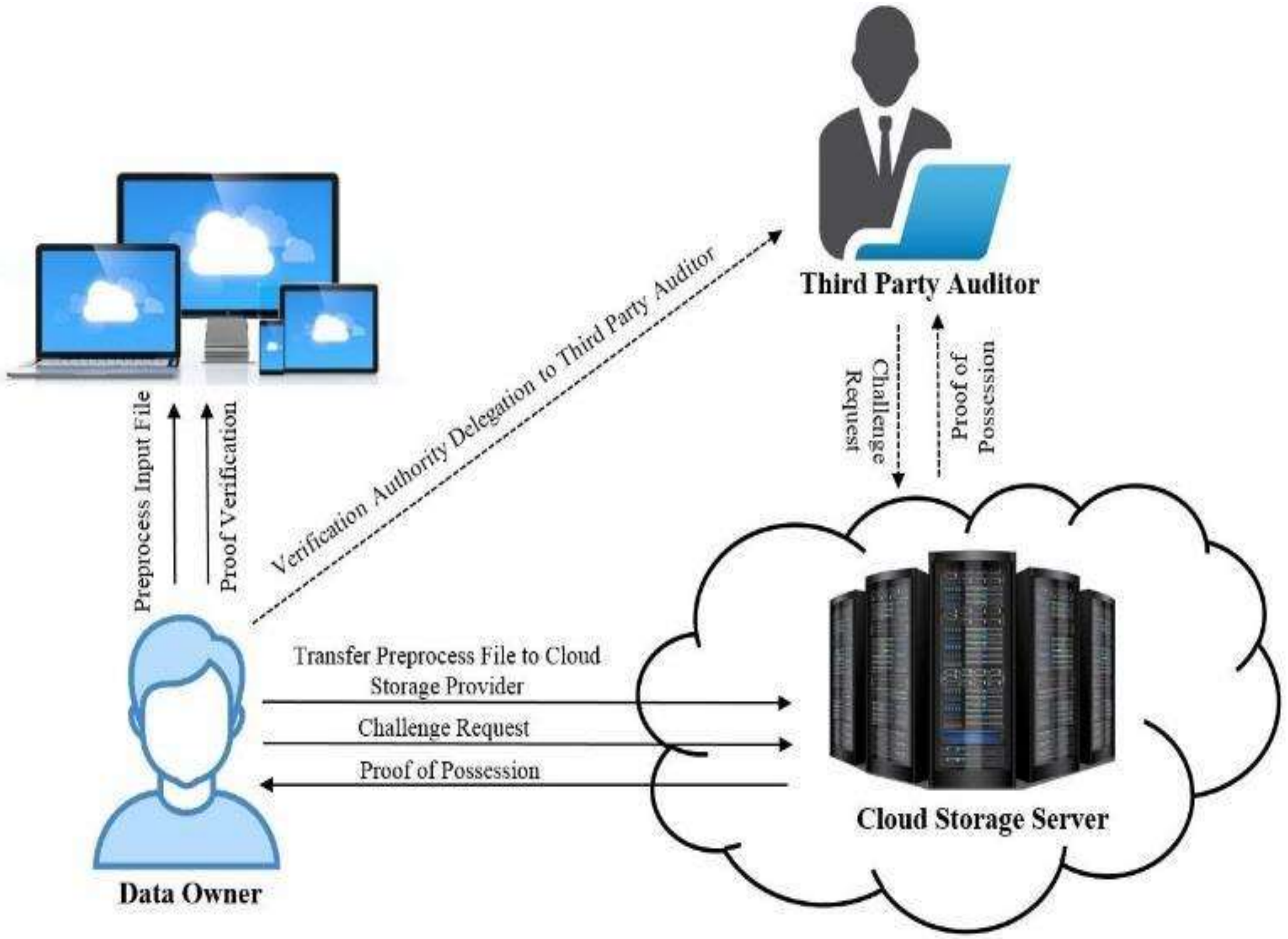
Security Challenges

Data Integrity

- Data integrity means ensuring that data is identically maintained during any operation (such as transfer, storage, or retrieval).

- Data integrity is assurance that the data is consistent and correct.

- Ensuring the integrity of the data really means that it changes only in response to authorized transactions.



Security Challenges

ImmatureTechnology

- In SaaS, the application must be developed in accordance with security standards.
- Most of the SaaS applications are web based therefore security is at most concern.
- The immature use of mashup technology (combinations of web services), is inevitably going to cause security vulnerabilities in those applications.
- SaaS development tool of choice should have a security model embedded in it to guide developers during the development phase and restrict users only to their authorized data when the system is deployed into production.
- As more and more mission-critical processes are moved to the cloud, SaaS suppliers will have to provide log data in a real-time.

Security Challenges

Constant Updation

- Cloud applications undergo constant feature additions, and users must keep up to date with application improvements to be sure they are protected.
- This means that users must constantly upgrade, because an older version may not function, or protect the data.
- Sensitive data is the domain of the enterprise, not the cloud computing provider.
- One of the key challenges in cloud computing is data-level security.

Security Challenges

Security Compliance

- Most compliance standards do not envision compliance in a world of cloud computing.

- There is a huge body of standards that apply for IT security and compliance, but not all translated to cloud.

- SaaS makes the process of compliance more complicated.

- Since it may be difficult for a customer to discern where its data resides on a network controlled by its SaaS provider, or a partner of that provider.

- Which raises all sorts of compliance issues of data privacy, segregation, and security.

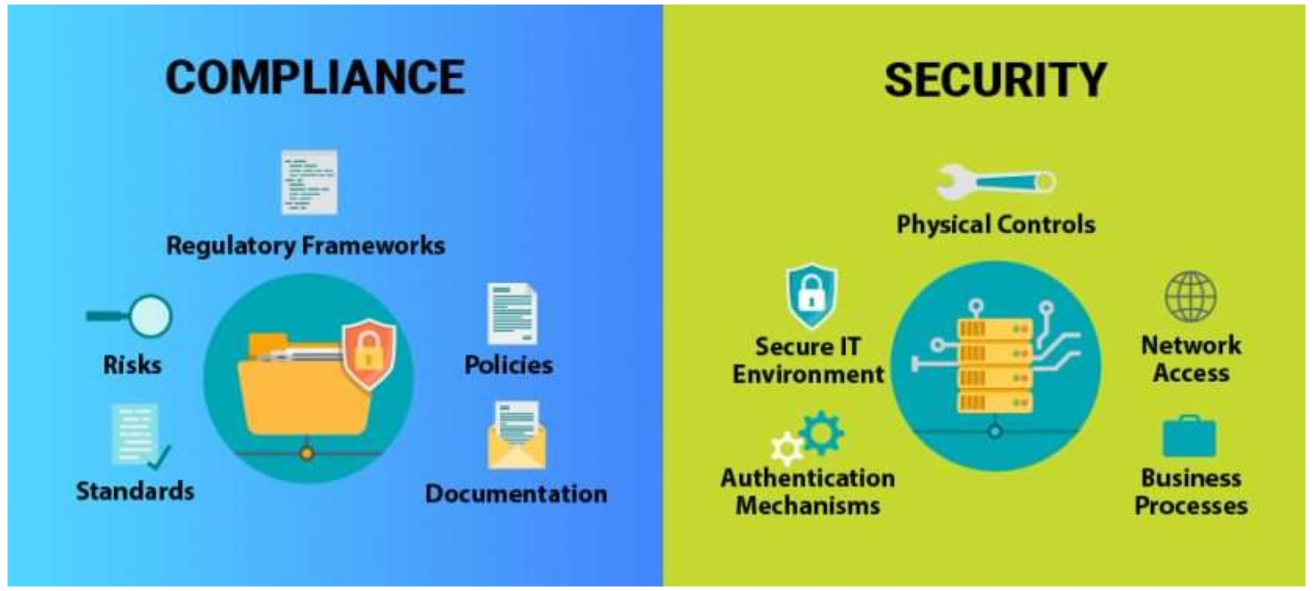
Security Challenges

Security Compliance

- Many compliance regulations require that data not be intermixed with other data, such as on shared servers or databases.

- Some countries have strict limits on what data about its citizens can be stored and for how long, and some banking regulators require that customers' financial data remain in their home country.

- There is a perception that cloud computing removes data compliance responsibility; however, it should be emphasized that the data owner is still fully responsible for compliance



Security Challenges

Virtualization

- Virtual machines will make it difficult to maintain the consistency of security and ensure the auditability of records.

- The ease of cloning and distribution between physical servers could result in the propagation of configuration errors and other vulnerabilities.

- Proving the security state of a system and identifying the location of an insecure virtual machine will be challenging.

- Regardless of the location of the virtual machine within the virtual environment, the intrusion detection and prevention systems will need to be able to detect malicious activity at virtual machine level.

THANK YOU