SNS COLLEGE OF TECHNOLOGY

(An Autonomous Institution)

Re-accredited by NAAC with A+ grade, Accredited by NBA(CSE, IT, ECE, EEE & Mechanical)
Approvedy by AICTE, New Delhi, Recognized by UGC, Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER APPLICATIONS

COURSE

23CAE717
Cloud Computing

UNIT V

SECURITY IN THE CLOUD

TOPIC

Security Overview – Cloud Security Challenges and Risks

Semester

II Semester / I MCA

Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.

"Set of control-based technologies and policies designed to follow to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use"
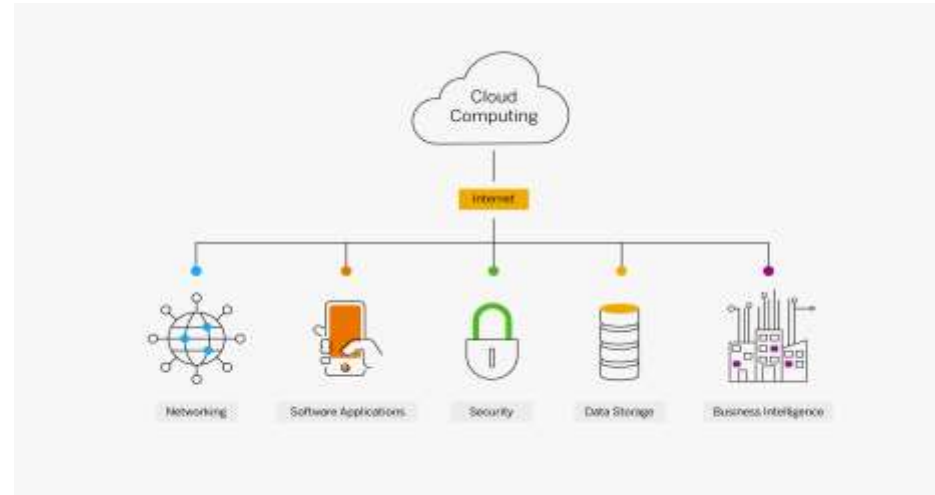
Concern on

- ❑ Identity management

- ❑ Access control

- ❑ Data security and Privacy

- ❑ Business continuity

- ❑ Data breach

- ❑ Backup plan
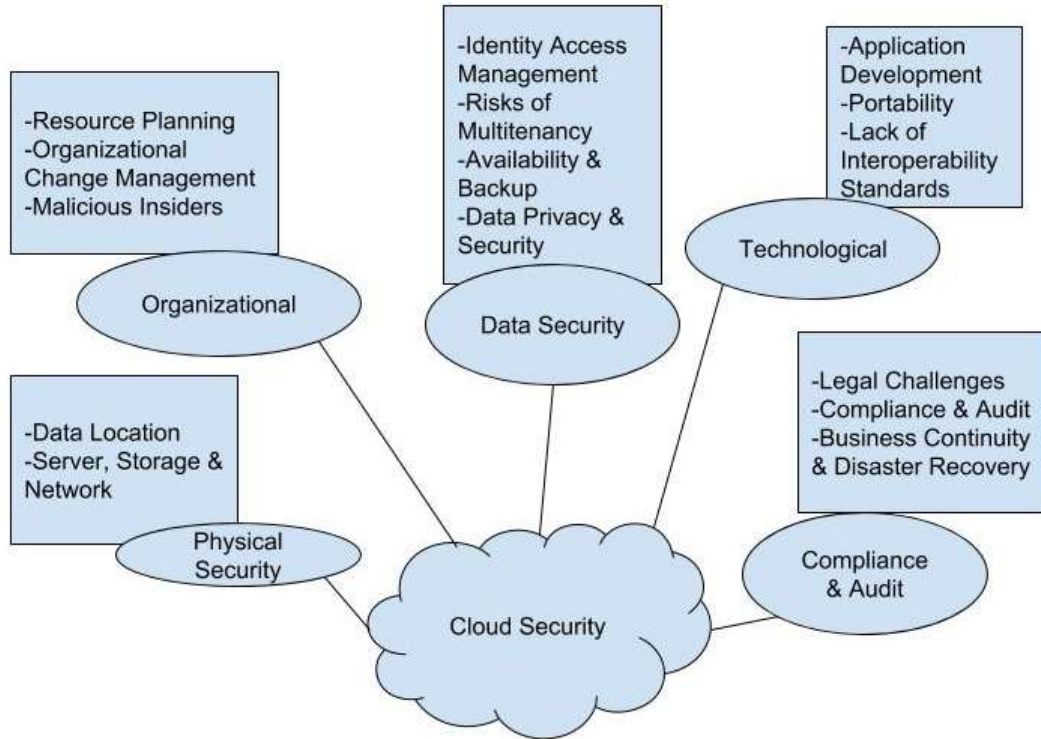
1. Data breaches

2. Insufficient identity, credential, and access management

3. Insecure interfaces and application programming interfaces

4. System vulnerabilities

5. Account hijacking

6. Denial of service

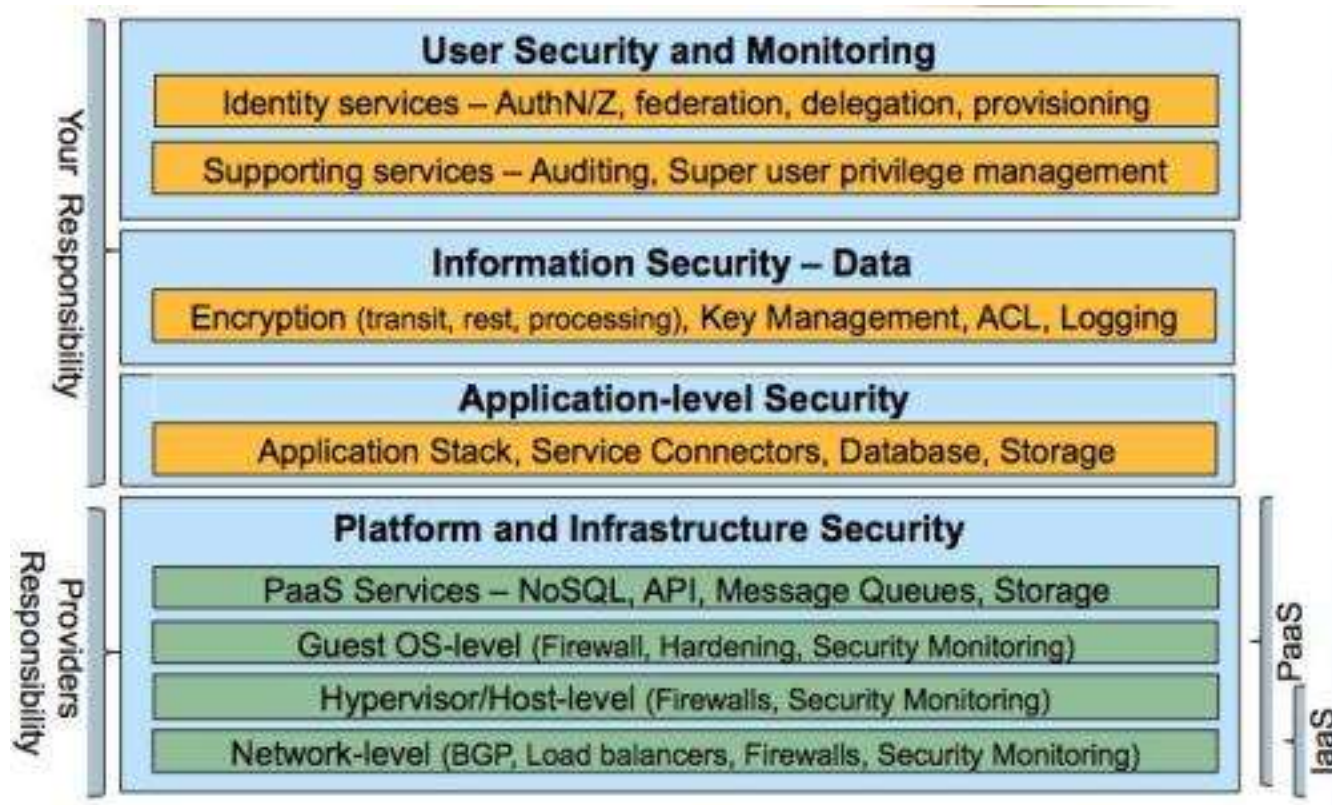7. Shared technology vulnerabilities

Your Responsibility

User Security and Monitoring
- Identity services – AuthN/Z, federation, delegation, provisioning
- Supporting services -- Auditing, Super user privilege management

Information Security – Data
- Encryption (transit, rest, processing), Key Management, ACL, Logging

Application-level Security
- Application Stack, Service Connectors, Database, Storage

Providers Responsibility

Platform and Infrastructure Security
- PaaS Services – NoSQL, API, Message Queues, Storage
- Guest OS-level (Firewall, Hardening, Security Monitoring)
- Hypervisor/Host-level (Firewalls, Security Monitoring)
- Network-level (BGP, Load balancers, Firewalls, Security Monitoring)

PaaS

IaaS

Cloud Security	Traditional IT Security
Third-Party Data Centers	In-House Data Centers
Low Upfront Infrastructure Investments	High Upfront Costs
Quickly scalable	Slow Scaling
Efficient Resource Utilization	Lower Efficiency
Reduced Time To Market	Longer Time To Market
Usage-Based Cost	Higher Cost

1. Data Protection – both in storage and transit

2. User Authentication – access logs

3. Possibility Planning – recovery

4. Service Provider Visibility

5. Attacks like virtual host confusion

6. Shadow IT - inability of IT to monitor the activities of the user

7. Resource location

8. Multitenancy issue

9. System monitoring and logs

10. Cloud standards

11. Service level agreements

Cloud Security

Cloud Security Issues

TOP 3 DATA SECURITY CONCERNS
FOR CLOUD SERVICES

#1 LACK OF CONTROL OVER THE LOCATION OF DATA
82% U.S.
56% OTHERS

#2 INCREASED VULNERABILITIES FROM SHARED INFRASTRUCTURE
79% U.S.
52% OTHERS

#3 PRIVILEGED USER ABUSE AT THE CLOUD PROVIDER
78% U.S.
56% OTHERS

49% DATABASES
39% FILE SERVERS
36% CLOUD
HIGHEST VOLUMES OF SENSITIVE DATA

40% CLOUD
39% MOBILE
38% DATABASES
MOST WORRIED ABOUT DATA ON

1. Verify Provider Compliance

- Authenticate compliance and governance practices.
- Review FedRAMP Security Packages to corroborate compliance claims.

2. Assume Proactive Role

- Advise providers to follow specific security procedures for laws like HIPAA.
- Train staff to use authorized services properly and to avoid unofficial data flows.

3. Understand Service Terms

- Some providers trawl your content to serve ads or analyze product usage.
- Use audit records and system-access logs to ensure your data is being maintained securely.

4. Conduct Routine Assessments

- Define or adopt your own set of standards for routine assessments.

Cloud Security Standards

1. EEE Cloud Computing Standard Study Group (IEEE CCSSG)

2. ITU Cloud Computing Focus Group

3. Cloud Security Alliance (CSA)

4. Distributed Management Task Force (DMTF)

5. Storage Networking Industry Association (SNIA)

6. Open Grid Forum (OGF)

7. Open Cloud Consortium (OCC) and Organization for the Advancement of Structured Information Standards (OASIS)
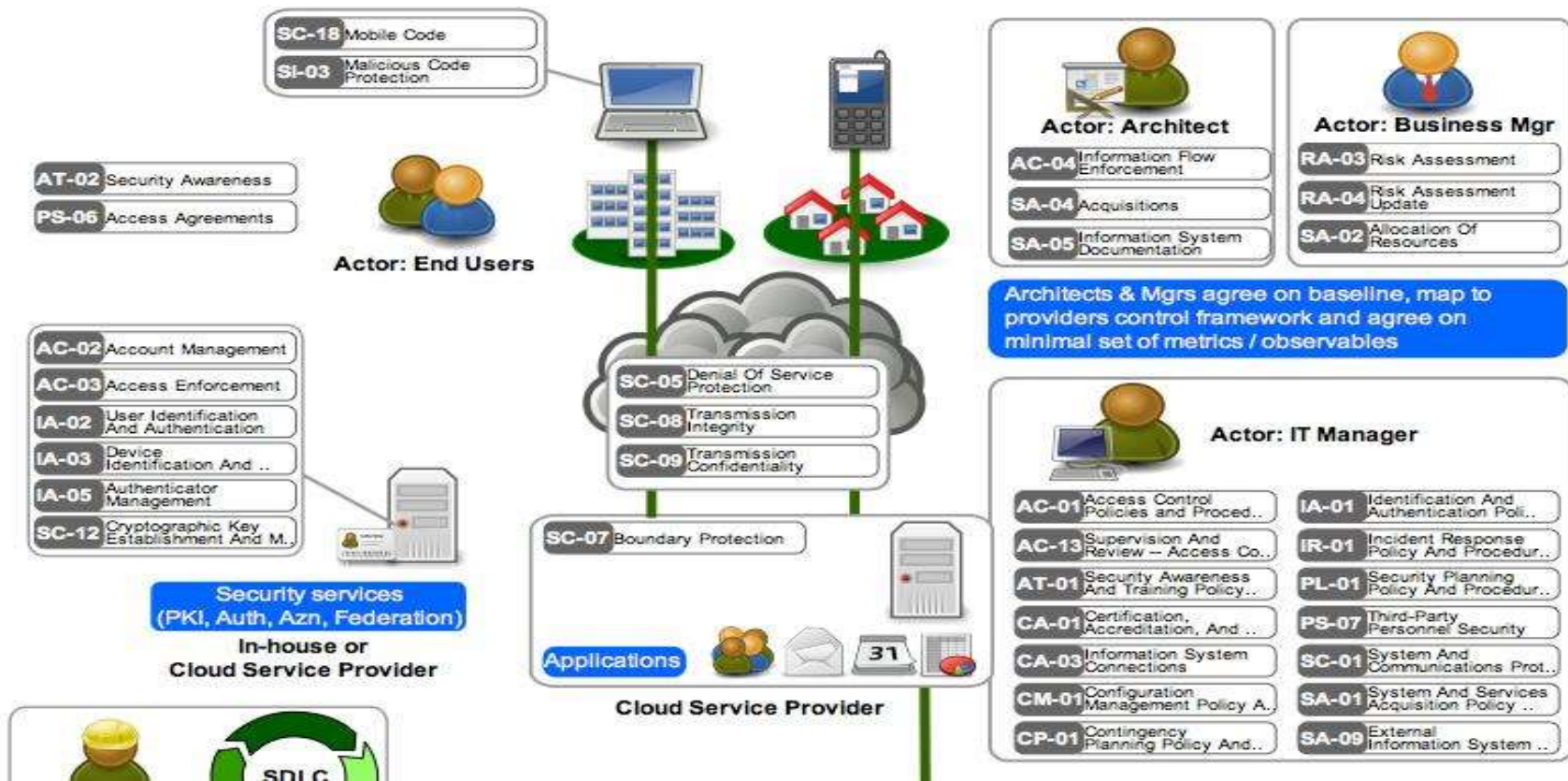
❑ Intercloud" standards in the following domains are needed to increase cloud interoperability and free data movement among clouds:

       ❑ Network architecture,

       ❑ Data format

       ❑ Metering and billing

       ❑ Quality of Service

       ❑ Resource provisioning

       ❑ Security, identity management and privacy

REFERENCES

❑ Kai Hwang, Geoffrey C Fox, Jack G Dongarra, "Distributed and Cloud Computing, From Parallel Processing to the Internet of Things", Morgan Kaufmann Publishers, 2012

❑ James E. Smith, Ravi Nair, "Virtual Machines: Versatile Platforms for Systems and Processes", Elsevier/Morgan Kaufmann, 2005.

❑ Kumar Saurabh, "Cloud Computing – insights into New-Era Infrastructure", Wiley India,2011.

❑ Toby Velte, Anthony Velte, Robert Elsenpeter, "Cloud Computing, A Practical Approach", TMH, 2009.

❑ John W.Rittinghouse and James F.Ransome, "Cloud Computing: Implementation, Management, and Security", CRC Press, 201

ANY QUERIES ?