Cloud Security and Forensics

Dr. Mukti Padhya
Assistant Professor, NFSU

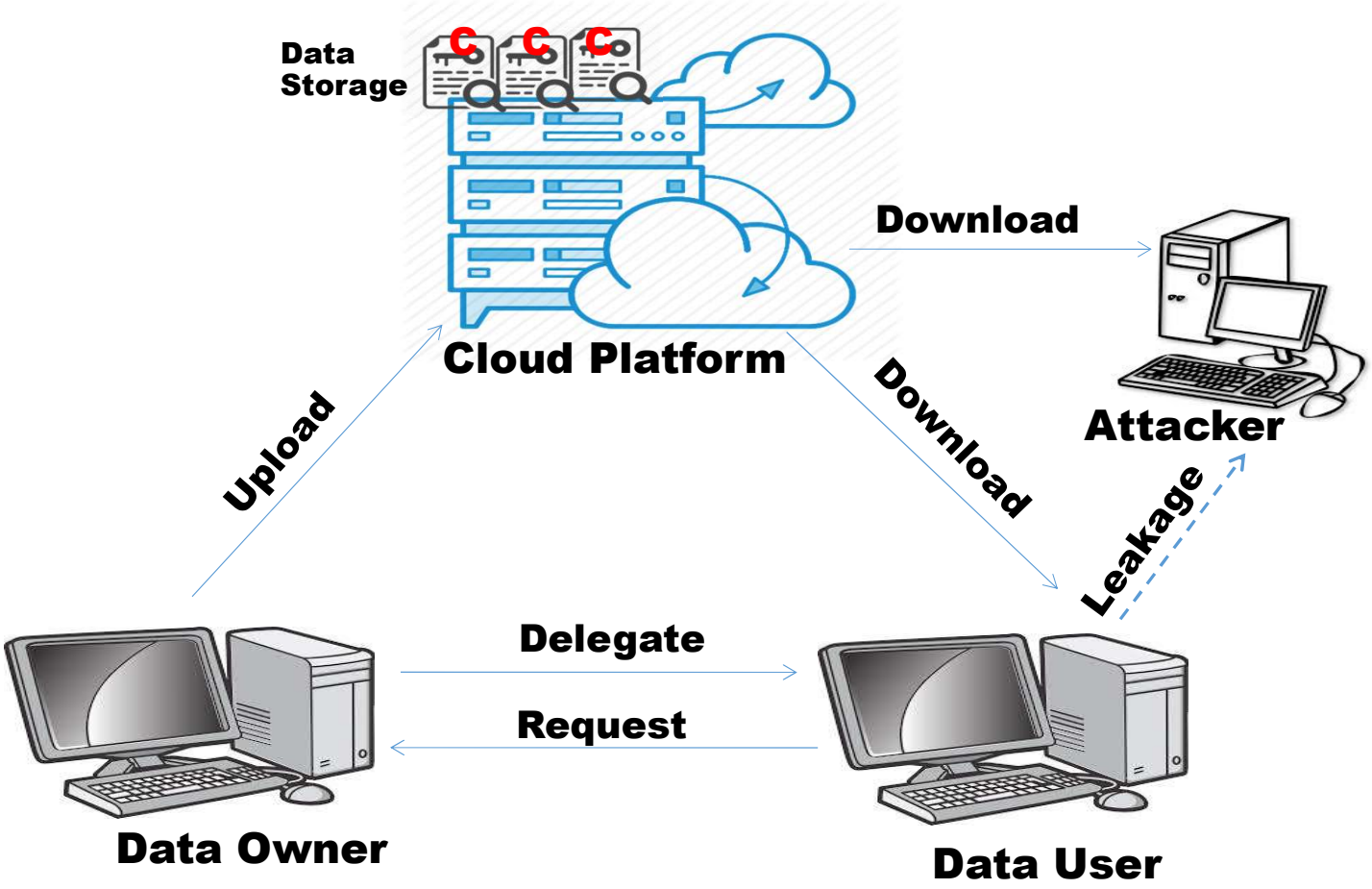
CTMSCS SIII P3 : Cloud Security and Forensics

- Subject Details
  - Teaching Scheme
    - Theory Credits : 3
    - Practical Credits : 1
  - Evaluatuion Scheme
    - Internal Exams
      - TA1/ TA2 (25 Marks Each)
      - MId Sem Exam : 50 Marks
    - End Sem Exam : 100 Marks
    - Practical End Sem Exam : 100 Marks

CTMSCS SIII P3 : Cloud Security and Forensics

- Understand key terms, concepts of cloud computing and security
- Explain the core concepts of the cloud computing paradigm: how and why this paradigm shift came about, the characteristics, advantages and challenges brought about by the various models and services in cloud computing.
- Understand basics principles of how cloud is built and operated
- Ability to understand existing cloud Infra
- Ability to identify, analyse, prevent security breaches in cloud scenario
- Develop policies to strengthen cloud security
- Cloud Forensics, Cloud Pen Testing

Cloud Services



Syllabus

- Unit – I Introduction
  - Recent trends in computing, evolution of cloud computing, Cloud computing (NIST model), properties, characteristics and disadvantages,
  - Layer and Types of Cloud,
  - Risk and Approaches of Migration into Cloud, Research challenges.
  - Cloud computing stack, Layer and Types of Cloud, Attacks and Vulnerabilities, Countermeasure,

- Unit – II Cloud Computing Architechture
  - Cloud Storages Types
  - Virtualization Technology : Virtualization Structure/ Tools, Mechanism, Implementation Level of Virtualization, Types
  - Hypervisor: VMWare, Xen, KVM
  - Virtual Cluster and Resource Management
  - Hypervisor memory optimization
  - Additional security features, Hardening the hardware management

Syllabus

- Unit – III Cloud Service Models
  - Cloud Service Models: PaaS, IaaS,SaaS, XaaS, BMaaS,
  - Deployment models: Public, Private, Hybrid
  - Service Management in Cloud
  - Service Level Agreements (SLAs), Billing & Accounting
  - Datacenter Design and Interconnection Network,
  - Cloud Logging Services
  - Log Collection and Analysis

- Unit – IV Securing Cloud Communication
  - Infrastructure security, Data security and storage,
    - Cryptography, Encryption Algo.,
  - Identity and Access Management, Access Control, Authentication in Cloud computing.
  - Trust and Reputation, PKI - Certificates, Digital Sign
  - API Security

- Unit – V Emerging Cloud Environments and Cloud Forensics
  - Cloud Forensics : Framework, Cloud Crime, Digital Forensics
  - Case Study on Open Source and Commercial Clouds: Emerging Cloud Environment, Eucalyptus Architecture, Open Nebula, Nimbus. Google App Engine (GAE), IBM Cloud, VM Ware cloud

The rising importance of cloud security

- The use of cloud tools has been steadily rising for several years, and now almost no business can operate without some form of cloud computing solution. Almost all organisations rely on this, with 94% reporting significant security improvements and 80% benefitting from operational advantages since adopting the cloud.
- However, figures from Statista show 33% of businesses described themselves as 'extremely concerned' about the security of public cloud, with a further 42% saying they are 'very concerned'. Just one per cent said they have no worries about the safety of these operations.
- This means security professionals with specialist expertise in cloud technologies are in extremely high demand among businesses across all sizes and sectors. As a result, this area is a great environment for anyone who wants to get into cyber security or advance their career and work with cutting-edge technology at the world's largest organisations.

Why Industry need cloud specialists

- Some of the biggest concerns raised by firms about their cloud environments are:
  - Risk of data loss/leakage
  - Privacy/confidentiality issues
  - Accidental exposure of credentials
  - Legal/regulatory compliance

- The biggest specific cloud security threats firms face as a result of these shortcomings are:
  - Misconfiguration of the cloud platform
  - Exfiltration of sensitive data
  - Unauthorised access to systems or applications
  - Insecure interfaces or APIs
  - External sharing of data

Job Roles

- Cyber Security Consultant
- Security Analyst
- Security Architect
- Security Engineer
- Risk Analyst

Cloud Security and Forensics : Takeaway

- IoT cloud
- AI-as-a-service platforms
- Blockchain-as-a-Service (BaaS)
- Cryptographic Cloud
- Social Network Data : Graph Structure -->Data Retrieval
- Green Computing , Edge Computing, Fog Computing
- Business Intelligence
  - Data Analytics in Cloud
  - ML in Cloud

Lab Practical & TA2 Project

Cloud Services : Healthcare Scenario