Cloud Security: Challenges, Vulnerabilities & Solutions

Class Presentation by
Akshay Gujjar

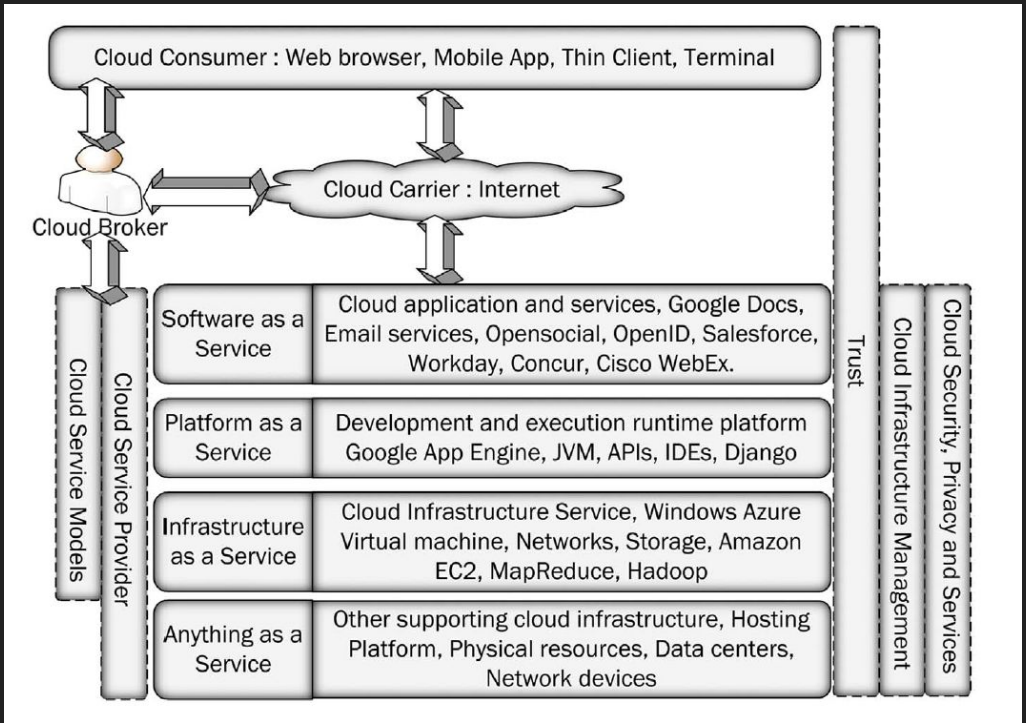
CECS 579
May 3, 2022

For further information, please contact: Akshay.Gujjar@student.csulb.edu

Cloud Computing

- Rapidly transforming IT landscape
- Access resources, applications and infrastructure
- Pay-as-you-use basis
- Massive Storage Infrastructure
- Increased flexibility
- Mobility
- Disaster Recovery
- Loss Prevention
- Automatic Software Updates
- Develop and deploy user applications

Service Models



[1] Singh, Ashish, and Kakali Chatterjee. "Cloud security issues and challenges: A survey." Journal of Network and Computer Applications 79 (2017): 88-115.

Deployment Models

- Private Cloud
  - Operated by a single organization
- Public Cloud
  - Run and managed by the cloud service provider
  - Cloud resources are shared among multiple people
  - Pay according to the services used
- Community Cloud
  - Shared by interest
- Hybrid Cloud
  - Combination of two or more clouds

Storage Models

- Shared File/Block Storage System
  - Shared among multiple users/hosts
  - Protocols used are Network File System (NFS), Server Message Block (SMB), and Common Internet File System (CIFS)
- Object Storage System
  - Data is stored/retrieved in the form of objects
  - Every object accessed by a global key, hash or Uniform Resource Locator (URL)
  - Uses Representational State Transfer (REST) or web based cloud services
- Database or table storage system
  - Data is stored in Relational Database Management Systems (RDBMs)
  - In the form of rows and columns

Cloud Security Concepts

- Virtualization Aspect
  - Process of extracting the services, applications, computing resources
  - Virtual Machines (VMs) and Virtual Machine Managers (VMMs) are components
  - A VM is an image of the operating system (OS) called guest OS
  - Guest OS runs multiple programs on it
  - No direct access to the hardware
  - VMMs are used for creation, deletion and allocation virtual resources to the VM
- Multi-tenancy
  - Sharing concept
  - Running instance shared by tenants
  - Single cloud platform shared among multiple users
  - In IaaS, VMMs refers to sharing platform, VMs refers to instances

Cloud Security Concepts

- Data Outsourcing
  - Data extraction and collection done by a third party
  - Provides data storage, data management, computing and security services
  - Creates a physical separation between the data owner and data
  - Security of data is a major concern

Requirements of Cloud Security

- The six security requirements
  - Authentication or identification
  - Authorization
  - Confidentiality
  - Integrity
  - Non-repudiation
  - Availability
- Each service model requires authorization for public cloud
- Public and private clouds require more security
- The six security requirements are essential for all cloud models

Threats to Cloud Computing

- Data loss and leakage
  - Deletion, alteration and theft of data
  - Loss of encoding key
  - Lack of authentication, authorization, access control, weak encryption algorithms, keys, etc.
  - Can affect all service models
  - Prevention methods include secure API, storage, data integrity, strong encryption key, etc
- Insecure interface and API
  - Software interfaces and APIs are provided by cloud providers
  - They provide provisioning, management, and monitoring services
  - Security of the cloud relies on the security of these APIs
  - Security of these APIs can be hampered due to accidents or malicious attempts
  - Can be prevented by proper authentication and access control mechanisms

Threats to Cloud Computing

- Identity Theft
  - Impersonation of identity, credits, resources of a legitimate user
  - The victim suffers unwanted results and losses
  - Causes are weak password recovery method, phishing attacks, keyloggers, etc.
  - Can be prevented by using multi-authentication, strong password recovery method

Attacks on Cloud Security

- Denial of Service Attack
  - Attacker sends thousands of request packets to the victim
  - Aim of the attacker is to exhaust all resources
  - Attacker floods a large number of requests to waste the computational power, performance time and cryptographic operations
- Distributed Denial of Service Attack (DDoS Attack)
  - More complex and harder to detect
  - Controller scans the whole network, lists out handlers
  - Handler recruits zombies to launch the attack
- Service Injection Attack
  - User sends a request to the cloud
  - Attacker makes a new malicious image of the requested service as a cloud service
  - Can be prevented by using a service integrity module

Cloud Security Issues and Solutions

- Data storage
  - Loss of control is a major issue
  - Hard to check data integrity and confidentiality
  - The user is physically separated from their data, storage and computing server
  - Organizations store the data on the basis of multi-location feature
- Un-trusted Computing
  - When an application calls another application or service, a service tree is generated
  - In large data sets, there may be inaccurate results
  - It is hard to find an accurate computation server
- Cryptography
  - Bad implementation of algorithm or weak key
  - Cryptosystems like RSA (Rivest–Shamir–Adleman) can be used

Cloud Security Issues and Solutions

- Internet and Services related Security Issues
  - Internet transmits a large number of packets from source to destination
  - It is unsafe because data is passed through a number of nodes
  - Issues like IP spoofing, port scanning, malware injections, and packet sniffing
  - The web and standard web browsers are not the safe
  - There are many solutions, but also newer problems

Conclusion

- Issues originate due to the public, shared, distributed and virtualized nature of the cloud
- Multi-tenancy and virtualization allow the users to access resources from different locations
- Cloud Computing is a rapidly emerging technology
- Widely accepted
- All users must be aware of the vulnerabilities, threats and attacks

References

[1] Singh, Ashish, and Kakali Chatterjee. "Cloud security issues and challenges: A survey." Journal of Network and Computer Applications 79 (2017): 88-115.

[2] I. Odun-Ayo, M. Ananya, F. Agono and R. Goddy-Worlu, "Cloud Computing Architecture: A Critical Analysis," 2018 18th International Conference on Computational Science and Applications (ICCSA), 2018, pp. 1-7, doi: 10.1109/ICCSA.2018.8439638.

[3] A. Behl, "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," 2011 World Congress on Information and Communication Technologies, 2011, pp. 217-222, doi: 10.1109/WICT.2011.6141247

[4] A. Bouayad, A. Blilat, N. E. H. Mejhed and M. El Ghazi, "Cloud computing: Security challenges," 2012 Colloquium in Information Science and Technology, 2012, pp. 26-31, doi: 10.1109/CIST.2012.6388058.