SK쉴더스 루키즈 26기 교육

Cloud computing security issues and responsibility sharing

Prof. Hyung-Jong(JOHN) Kim
hkim@swu.ac.kr

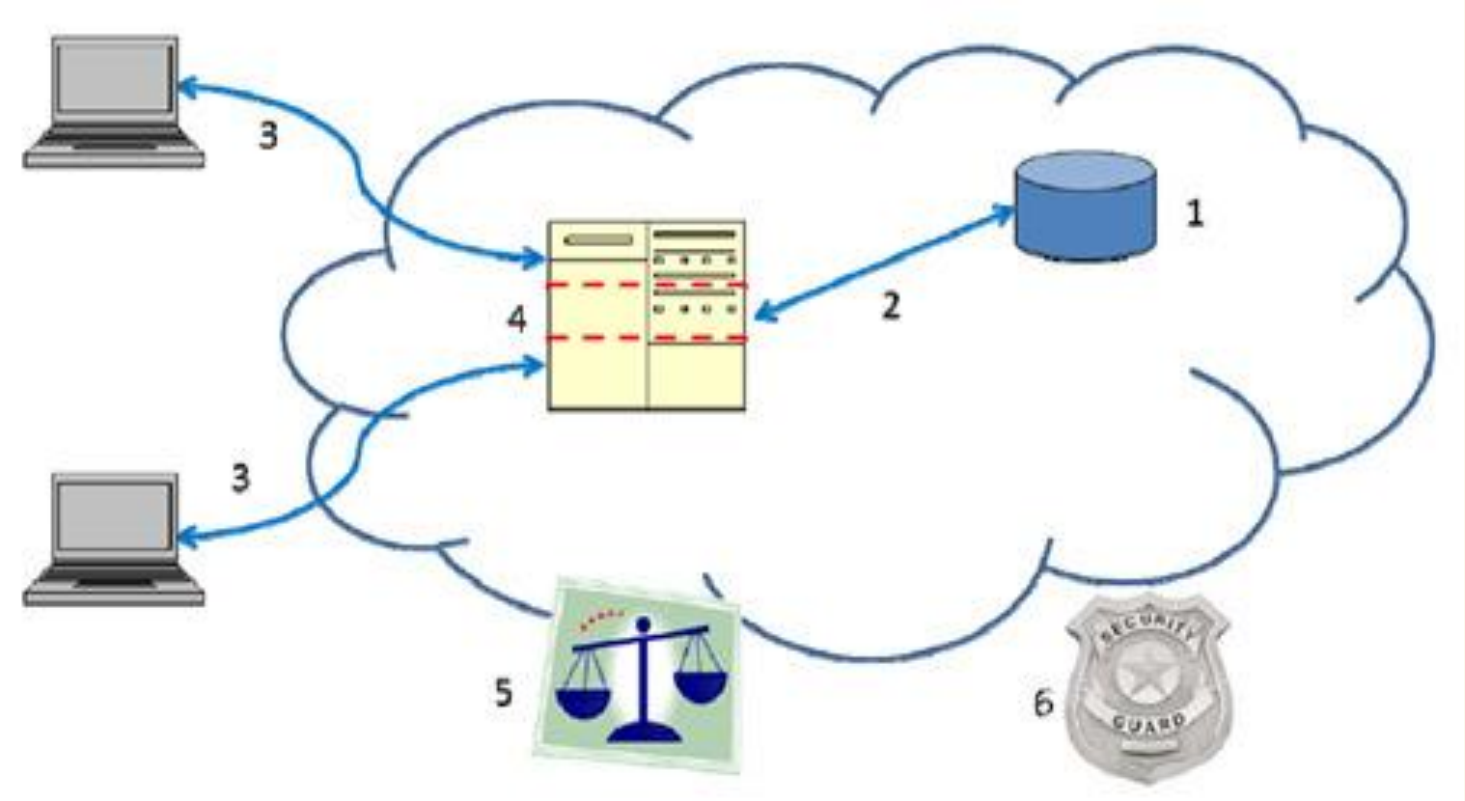
Dept. of Information Security
Seoul Women's University

Overall View of Cloud Computing Security

(1) security of data at rest

(2) security of data in transit

(3) authentication of users/applications/ processes

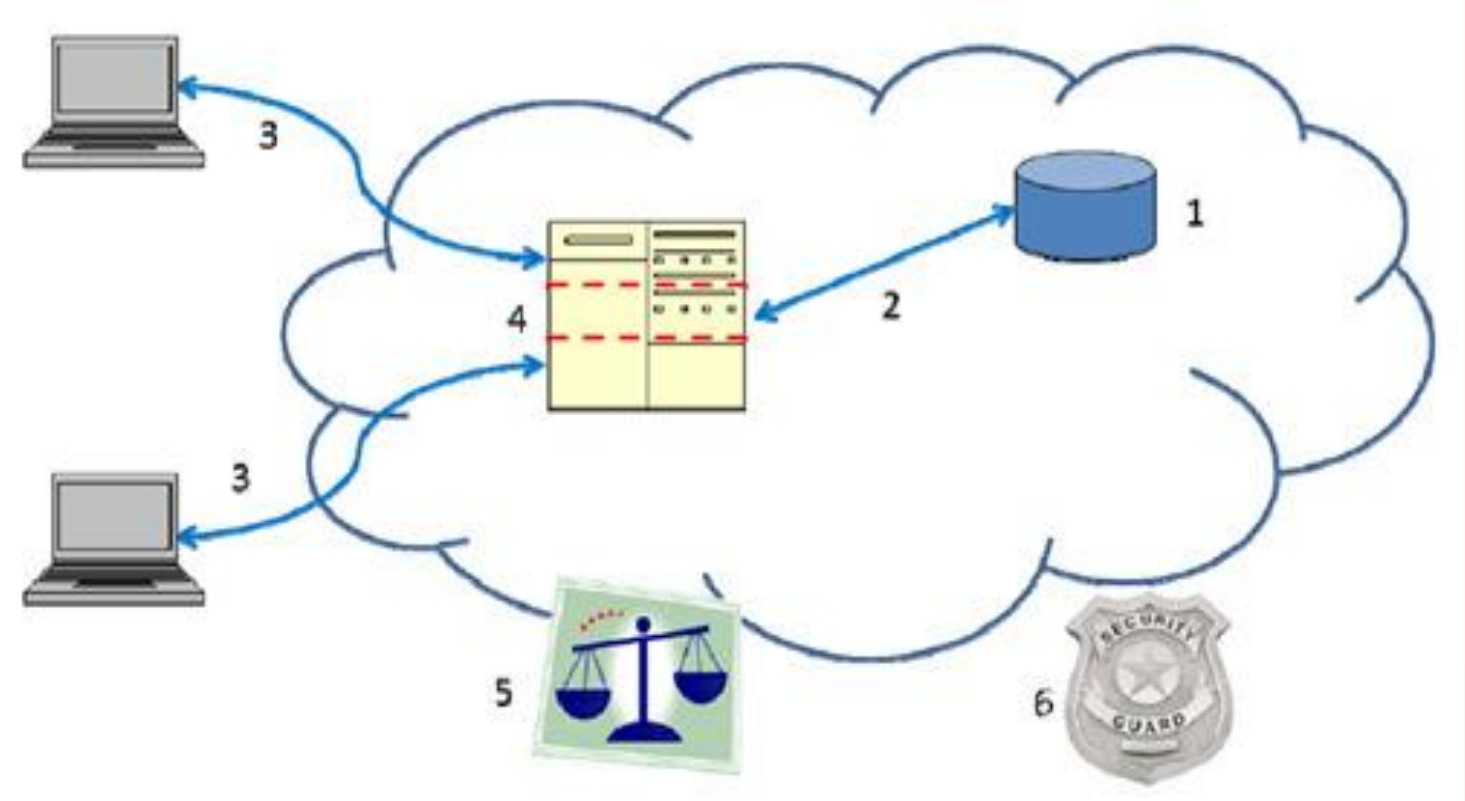


Overall View of Cloud Computing Security

(4) robust separation between data belonging to different customers

(5) cloud legal and regulatory issues

(6) incident response.



For securing data at rest

- **Cryptography tools** should be applied
  - For the confidentiality and integrity of data.
- **Redundancy of data** could be guaranteed.
  - For preserving availability,
- Responsibility on users
  - IaaS
- CSP has roles on this area
  - PaaS and SaaS

For security of the data in transit

- Cryptography technology would be the essential
  - for preventing from eavesdropping and manipulating.
- Among the virtual machines within a cloud, users may think it is relatively safe.
  - Not easy to guarantee that the traffic would not go through public internet. (ex. Multi-cloud deployment model)
- Between user's pc and cloud server
  - Inevitably go through public internet
  - Relatively risky and countermeasures are required

Authentication of users/applications/ processes

- User's end system to the cloud environment management console
  - only legitimate access from outside of the cloud.
- The majority of cloud services
  - web-based access as their gateway of computing resource.
- The web site for accessing the cloud service is publicly located
  - the access to the web is specially managed and controlled
  - well-defined authentication mechanism

Robust separation between data belonging to different customers

- When a physical system is used for deploying several virtual machines
  - The computing resource of the one virtual machine should not be disclosed to the other virtual machines.
- The multi-tenancy characteristic of cloud computing environment
  - Cloud service provider need to guarantee the independent operation of each virtual machine.
- Two aspects
  - Preserving secrecy of data
  - Concealing side channel

cloud legal and regulatory issues

- Cloud computing services can arouse legal issues,
  - when a company decide to transfer their information asset to cloud environment.
- The information can be stored in different country
  - how to handle possible disputes.

incident response

- Incidents take place on computing resources which can be located in remote places
  - the damage is supposed to be on users.
- Effective procedures which users and cloud service providers are participating together.
  - Incident alarms
  - Sharing the logs and evidences with users
- Utilizing functions from cloud services for incident responses
  - Load balancing, Fault domain and auto scaling

Responsibility Sharing in Cloud

- **Tesla vs AWS**

LILY HAY NEWMAN SECURITY 02.20.2018 05:06 PM

Hack Brief: Hackers Enlisted Tesla's Public Cloud to Mine Cryptocurrency

The recent rash of cryptojacking attacks has hit a Tesla database that contained potentially sensitive information.

CRYPTOJACKING ONLY REALLY coalesced as a class of attack about six months ago, but already the approach has evolved and matured into a ubiquitous threat. Hacks that co-opt computing power for illicit cryptocurrency mining now target a diverse array of victims, from individual consumers to massive institutions—even industrial control systems. But the latest victim isn't some faceless internet denizen or a Starbucks in Buenos Aires. It's Tesla.

Researchers at the cloud monitoring and defense firm RedLock published findings on Tuesday that some of Tesla's Amazon Web Services cloud infrastructure was running mining malware in a far-reaching and well-hidden cryptojacking campaign. The researchers disclosed the infection to Tesla last month, and the company quickly moved to decontaminate and lock down its cloud platform within a day. The carmaker's initial investigation indicates that data exposure was minimal, but the incident underscores the ways in which cryptojacking can pose a broad security threat—in addition to racking up a huge electric bill.

https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/

Responsibility Sharing in Cloud

- **Tesla vs AWS**
  - Hijacking AWS cloud system – Kubernetes console without security countermeasures
  - AWS credentials were revealed and the hackers made use of the credentials to mine the crypto currency
  - How to conceal?
    - Lowering the CPU usages
    - Hiding the servers behind the Cloudflare
  - The thing we need to think over
    - Did AWS provide the secure environment?
    - Did Tesla check the security requirement from AWS and set security configuration properly?

Responsibility Sharing in Cloud

- **Tesla vs AWS**
  - Your thought?
    - AWS should do something for handling the anomalies.
    - Tesla should do something for limit the abnormal access trials with the proper configuration
    - Both of them should do something
  - The Tesla has more responsibility on this issues
    - Because Amazon EKS console's IAM mechanism should be applied by the users
    - Attackers hid real IP address of attackers using CloudFlare and lowered the usages computing resources
  - However, CSP also needs to do something for the users -Detection and prevention of the anomalies using AI kind of technologies.

Responsibility Sharing in Cloud

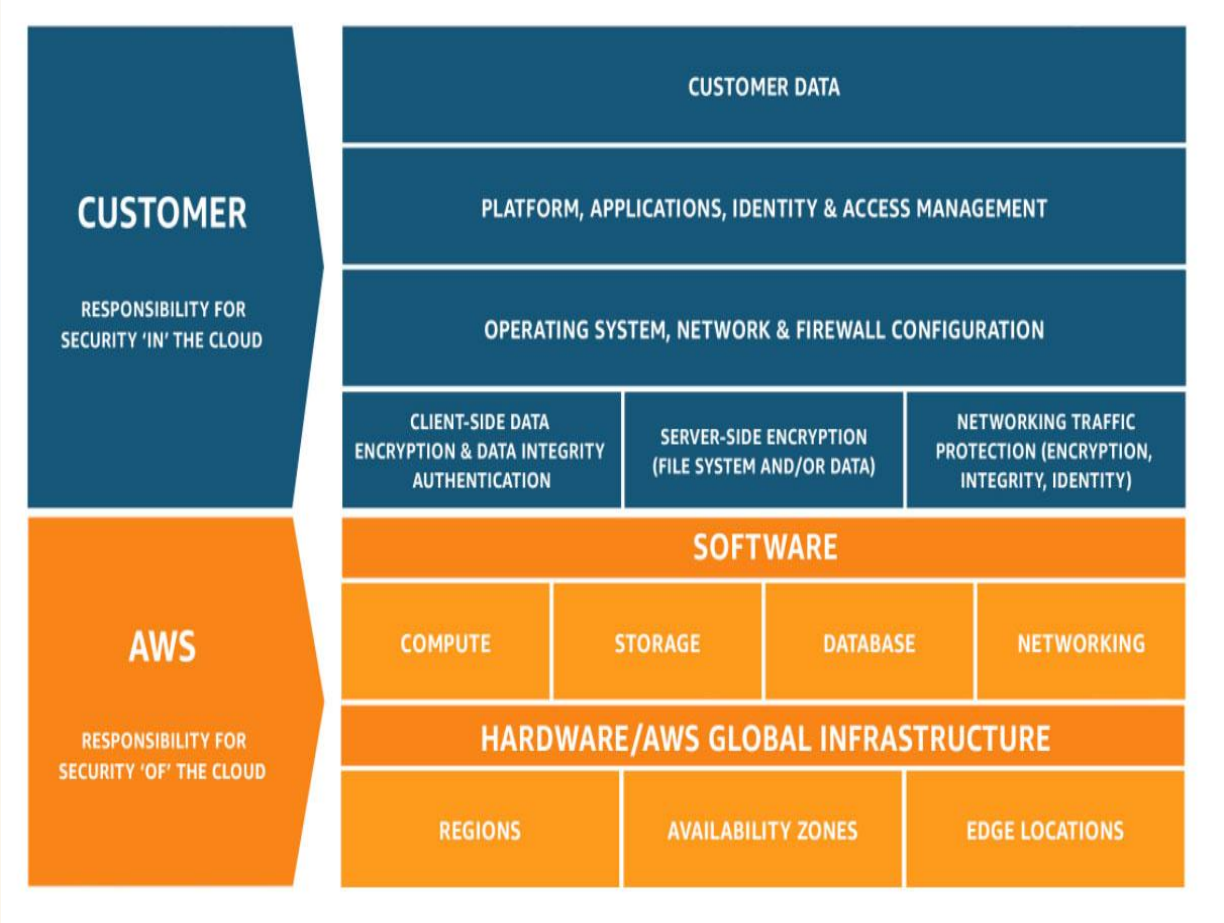
- Layers of the cloud computing services
  - From data to networking
- Responsibilities can be defined by
  - Configurable or not?
  - Manageable or not?
- What sharing means?
  - Not for passing the buck
  - But for clarifying the roles

Responsibility Sharing in Cloud

- On-premises case
  - Companies (not CSP) need to hire engineers with the expertise on virtualization and pooling resources
  - Virtualization and PR
    - New areas in system and network management
- IaaS/PaaS and SaaS
  - There could be reasonable boundary in responsibility share
  - Predefine the boundaries in SLA
  - Possible disputes or argument between users and CSPs

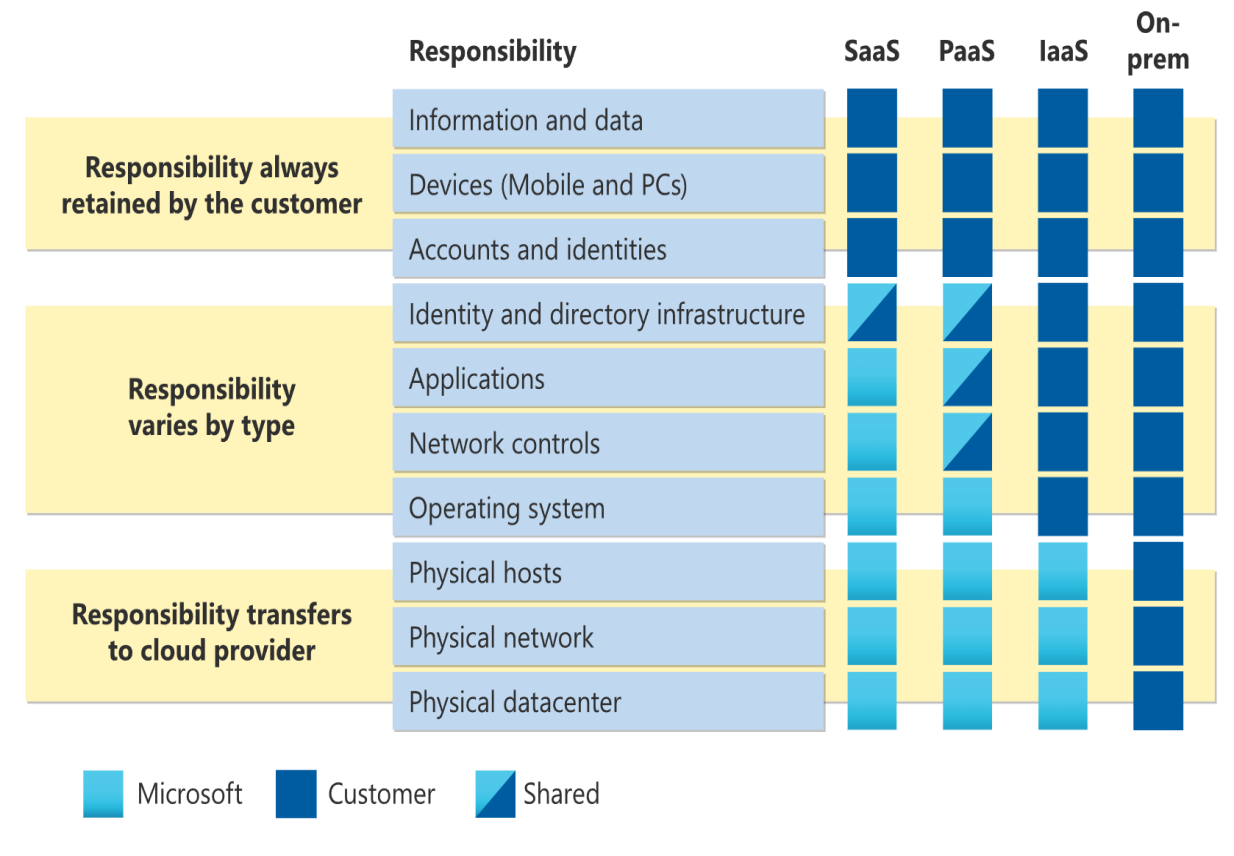
Responsibility Sharing in Cloud

- Amazon Web Services
  - Customers
    - Security in the cloud
    - In EC2 case – Access Managemnt, Operating system, Platform, Apps, Traffic filtering, encryption/decryption and so on.
    - In S3 case - Access Management, encryption/decryption of data,
  - AWS
    - Security of the cloud
    - Physical system/infra. management
      - Regions, az, edge location
    - Cloud software components security management
      - Compute, storage, DB, network



Responsibility Sharing in Cloud

- Microsoft Azure
  - In the IaaS case, there is a clear boundary
  - In the SaaS and PaaS case, the customers do not need to care the Operating System
  - In PaaS, there are shared parts in network controls, applications and identity and directory infra.
  - In SaaS, only the identity and directory infra is the area that the responsibility is shared



Responsibility Sharing in Cloud

- Microsoft Azure
  - Various alternatives for handling the responsibility related to security
  - Customers can transfer their responsibility to the CSPs by re-allocating resources
  - Leverage cloud-based security capabilities for more effectiveness
  - Make use of the cloud intelligence for security
  - Sharing the responsibilities