HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

# Security Mechanisms for Cloud Computing

## Masters Seminar WiSe 2020/21

Lecturer: Prof. Dr. Christopher Meinel

Tutors: Muhammad Sukmana

# Introduction

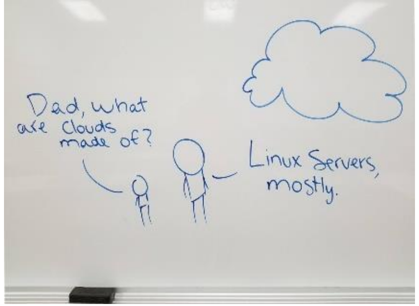
- Chair: Internet Technologies and Systems (Prof. Dr. Christoph Meinel)
- Tutors: Muhammad Sukmana
- Keywords: cloud computing, data protection, cloud security, access control, security risk analysis, threat detection
- Hands-on software development seminar

# Introduction

- Goal: *Implement contemporary mechanisms for security in the cloud.*
- Learning goals
  - Teamwork
  - Hands-on software development skills
  - Scientific writing
- Additional opportunities
  - Contribution to a real world project
  - Insight into contemporary challenges and solutions in cloud computing

# Introduction
## Cloud Computing

- General term for technologies for delivering hosted services over Internet
- The backbone of most services in the Internet
  - 85% of enterprise data is saved in the cloud
  - 67% of enterprise will move their infrastructure to the cloud by 2020
- Several reasons why most businesses move to the cloud
  - Better flexibility with a lot of services provided
  - Guaranteed to be always available
  - On-demand resources
  - Less maintainance cost compared to on-premise infrastructre



# Introduction
## Security Challenges in Cloud Computing

- The cloud has become a lucrative target for the attackers due to the growing adoption of cloud technologies
- Enterprise workloads including important and sensitive information is now retained in the cloud
- Cloud Security Alliance recently delivered a report of cloud computing‘s top threats, which includes:
  - □ Data breaches
  - □ Misconfiguration and inadequate change control
  - □ Insider threat
  - □ Limited cloud usage visibility

# CloudRAID Project

- Idea
  - Making public cloud storage securely accessible
  - Applicable to private user or enterprise scenarios
  - Apply proven concept to a new technology: RAID
  - Combine benefits of enhanced security and availability

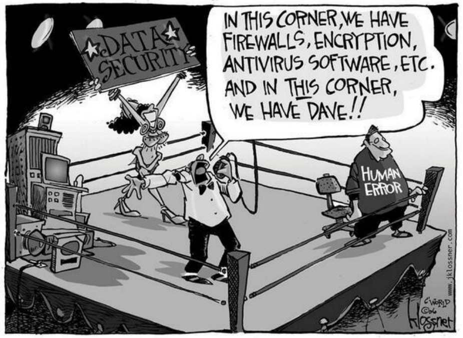
- Current Work
  - Started in May 2014 as research project in cooperation with Bundesdruckerei GmbH
  - Currently developed as enterprise storage solution by neXenio GmbH called Bdrive
  - Focus on continuous research support & creative ideas with proof-of-concept

More information: https://hpi.de/en/meinel/security-tech/cloud-security/cloudraid.html
https://www.bdrive.team/

# Seminar Task – Task 1

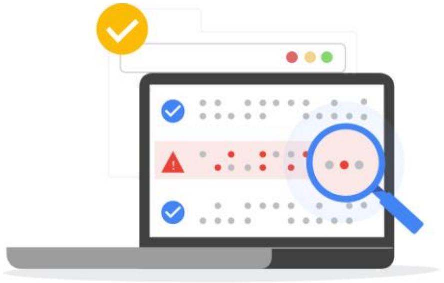
## Security Management in Multi-Cloud Environments

- Each cloud provider could have different ways of providing compute service that includes VMs, containers, networking, and IAM
- A cloud service may use the compute services from multiple cloud providers (e.g. AWS, Google Cloud)
- Cloud consumer currently can only manage and configure their resources using the management platform of each cloud provider
- Computing resource could be misconfigured due to human error that allows unauthorized user to access the important data
- Cloud consumer could configure their resources by not following the security best practice


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

# Seminar Task – Task 1
## Security Management in Multi-Cloud Environments

- Develop a security management platform for computing service in multi-cloud scenario:
  - Gather information of the computing resources and its configuration from multiple cloud providers (VM, container, networking, IAM)
  - Check if the configurations follow the best security practice
- Improve our proof-of-concept multi-cloud management platform
- Design and prototype implementation of the system

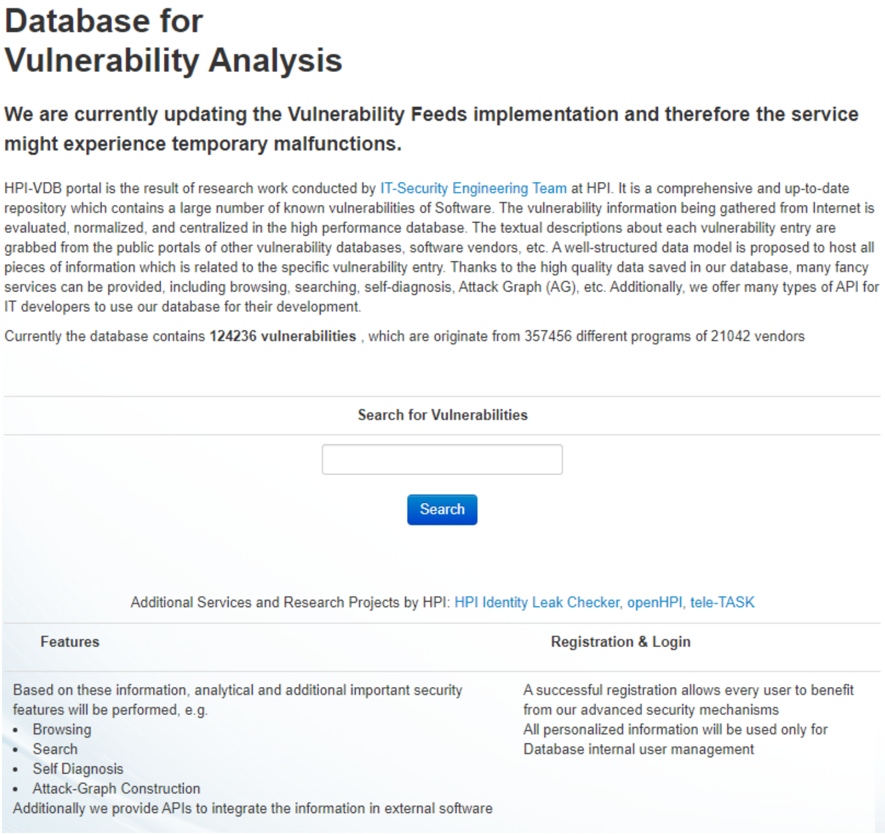


# Seminar Task – Task 2
## Vulnerability Database

- Nowadays, more vulnerabilities are discovered in various computer aspects due to insecure coding, bugs, or improper configurations
- Vulnerabilities can be exploited by attackers to gain authorized access to the resources that are unauthorized to them → “hacking‟
- Common Vulnerabilities and Exposures (CVE) is used to identify the discovered vulnerability, the level of exposure, and the remediation
- Vulnerability database services are important to identify and manage vulnerabilities in the system where it aggregates vulnerability information from multiple sources to be used for vulnerability scanning

# Seminar Task – Task 2
## Vulnerability Database

- HPI already has vulnerability database service (VDB) that can be accessed via hpi-vdb.de
- Automatically and periodically vulnerability information from the National Vulnerability Database (NVD) and Mitre
- Show basic information of vulnerabilities
- However, due to format change currentlz the service is not up-to-date



### Database for Vulnerability Analysis

**We are currently updating the Vulnerability Feeds implementation and therefore the service might experience temporary malfunctions.**

HPI-VDB portal is the result of research work conducted by IT-Security Engineering Team at HPI. It is a comprehensive and up-to-date repository which contains a large number of known vulnerabilities of Software. The vulnerability information being gathered from Internet is evaluated, normalized, and centralized in the high performance database. The textual descriptions about each vulnerability entry are grabbed from the public portals of other vulnerability databases, software vendors, etc. A well-structured data model is proposed to host all pieces of information which is related to the specific vulnerability entry. Thanks to the high quality data saved in our database, many fancy services can be provided, including browsing, searching, self-diagnosis, Attack Graph (AG), etc. Additionally, we offer many types of API for IT developers to use our database for their development.

Currently the database contains **124236 vulnerabilities** , which are originate from 357456 different programs of 21042 vendors

**Search for Vulnerabilities**

Additional Services and Research Projects by HPI: HPI Identity Leak Checker, openHPI, tele-TASK

**Features**

Based on these information, analytical and additional important security features will be performed, e.g.

- Browsing
- Search
- Self Diagnosis
- Attack-Graph Construction

Additionally we provide APIs to integrate the information in external software

**Registration & Login**

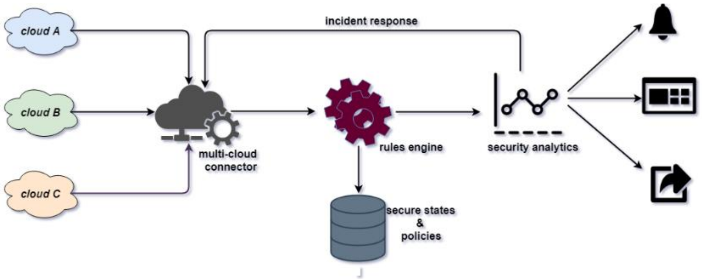
A successful registration allows every user to benefit from our advanced security mechanisms
All personalized information will be used only for Database internal user management

# Seminar Task – Task 2
## Vulnerability Database

- Periodically collect and aggregate vulnerability information from multiple sources, such as:
  - MITRE, National Vulnerability Databases
  - Operating system vulnerability database
  - Cloud computing security best practices
- Manage the vulnerability information that can be used by relying vulnerability scanner systems
- Design and prototype implementation of the system

# Seminar Task – Task 3
## Cloud Threat Detection and Incident Response

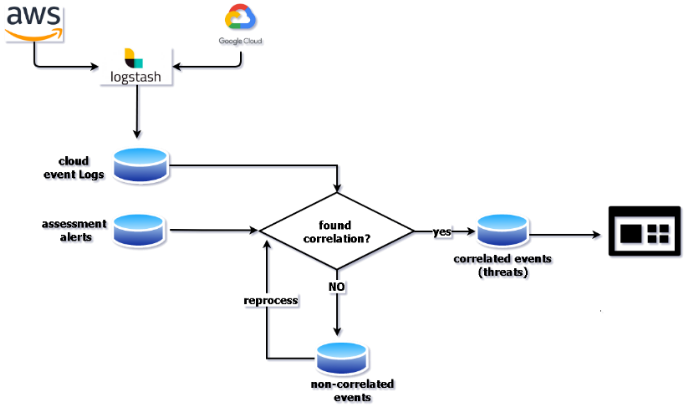
- Security monitoring is a fundamental aspect of threat detection to secure cloud resource
- Cloud activity logs generated by cloud providers are often ignored or not leveraged by cloud consumer
- Logs are downloaded, aggregated, processed, and analysed by the cloud consumers extract security relevant information
- If threats are detected, it should take necessary actions to secure the cloud resource



# Seminar Task – Task 3

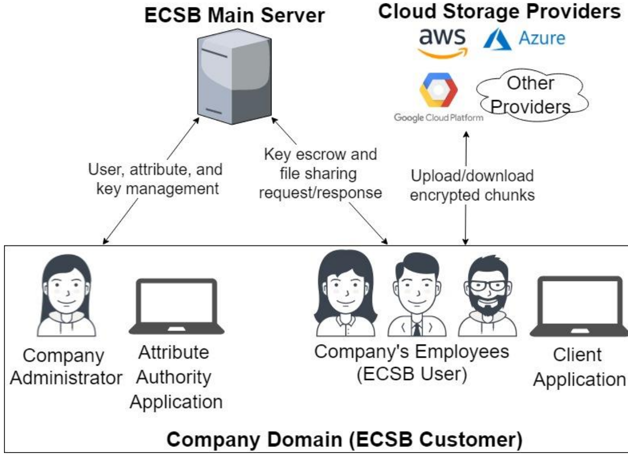
## Cloud Threat Detection and Incident Response

- Improve on our existing work of cloud log analysis system
- Build a security analytics pipeline prototype for analyzing cloud log activity
- Develop security analysis mechanisms & use cases to detect suspicious/malicious activities in the log
- Aggregate log with the alerts generated by cloud assessment application
- Respond to the detected incident/threats at the cloud assets
- Design and prototype implementation of the system



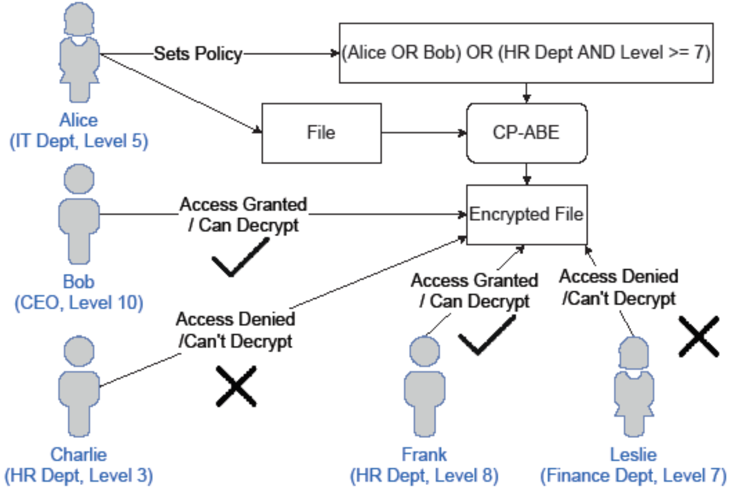
# Seminar Task – Task 4
## Secure Inter-Company File Sharing

- Enterprise file sharing solution, such as Enterprise Cloud Storage Brokerage (ECSB), might need to provide secure file sharing between companies for collaboration
- However, some challenges need to be faced by ECSB in order to provide secure and efficient file sharing
  - Access control: ECSB needs to provide organizational-based access control to avoid cross-company data leakage
  - Flexibility: The file sharing in the system should be flexible following user`s file access restriction specification


ECSB Main Server
Cloud Storage Providers
aws
Azure
Google Cloud Platform
Other Providers
User, attribute, and key management
Key escrow and file sharing request/response
Upload/download encrypted chunks
Company Administrator
Attribute Authority Application
Company's Employees (ECSB User)
Client Application
Company Domain (ECSB Customer)

# Seminar Task – Task 4
## Secure Inter-Company File Sharing

- We have developed a proof-of-concept ECSB based on an attribute-based encryption (ABE) scheme
- ABE is a new and experimental public key cryptography scheme that utilizes attributes as the keypair and the policy containing the attributes and logic gates
- Only authorized user with the correct attributes that fulfill the policy could decrypt the ciphertext
- The scheme has the flavour of multi-authority ciphertext-based policy ABE (CP-ABE)



# Seminar Task – Task 4
## Secure Inter-Company File Sharing

- Improve our proof-of-concept enterprise file sharing system available at https://github.com/Anroc/PAD-TFDAC-MACS
  - Provide system-level organizational-based access control for each company while allowing the company to access some files of other companies
  - Improve on the policy structure of the ABE scheme to ensure flexible file sharing in the system
- Design and prototype implementation of the system

# Organization (1/2)

- Working style
  - Groups up to 4 students @ group
  - Development of ideas to approach a given challenge
  - Design & implementation of a software solution
  - Option of on-site or online meeting via Zoom
- Deliverables
  - Presentations: initial (ideas), final (results)
  - Source code of proof-of-concept implementations
  - Technical report (6+ Pages, IEEE, 2 columns)

# Organization (2/2)

- Enrollment
  - □ Deadline: **Wednesday November 11th 2020**
  - □ Limit of **12 students** → first come first served
  - □ Via e-mail: muhammad.sukmana@hpi.de
  - □ Indicate your choice of task/group → first come first served
  - □ Need to sign NDA
- Lectures & Consultations
  - □ Lectures: occasionally on Fridays 9.15 a.m. – 10.45 p.m. in H-E 11
    - – Next lecture: **November 13th 2020**
  - □ Consultations: On demand H-1.18

Thank you
for your attention!

Muhammad Sukmana (muhammad.sukmana@hpi.de)
Kennedy Torkura (kennedy.torkura@hpi.de)