HPCC 2015, August 24 - 26, New York, USA

User-Controlled Security Mechanism in Data-Centric Clouds

Wei Chang[c]

Joint work with

***Qin Liu**[a]**, Guojun Wang**[b]**, and Jie Wu**[c]*

a. Hunan University, P. R. China
b. Central South University, P. R. China
c. Temple University, USA

Aug. 25, 2015

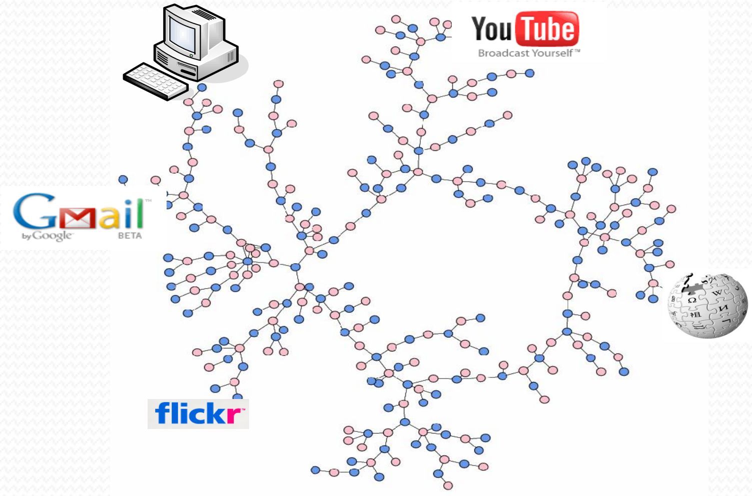
Outline

- Introduction to Cloud Computing
- Security Issues in Cloud Computing
- Data-Centric Security
- User-Controlled Security Mechanism
- Conclusion

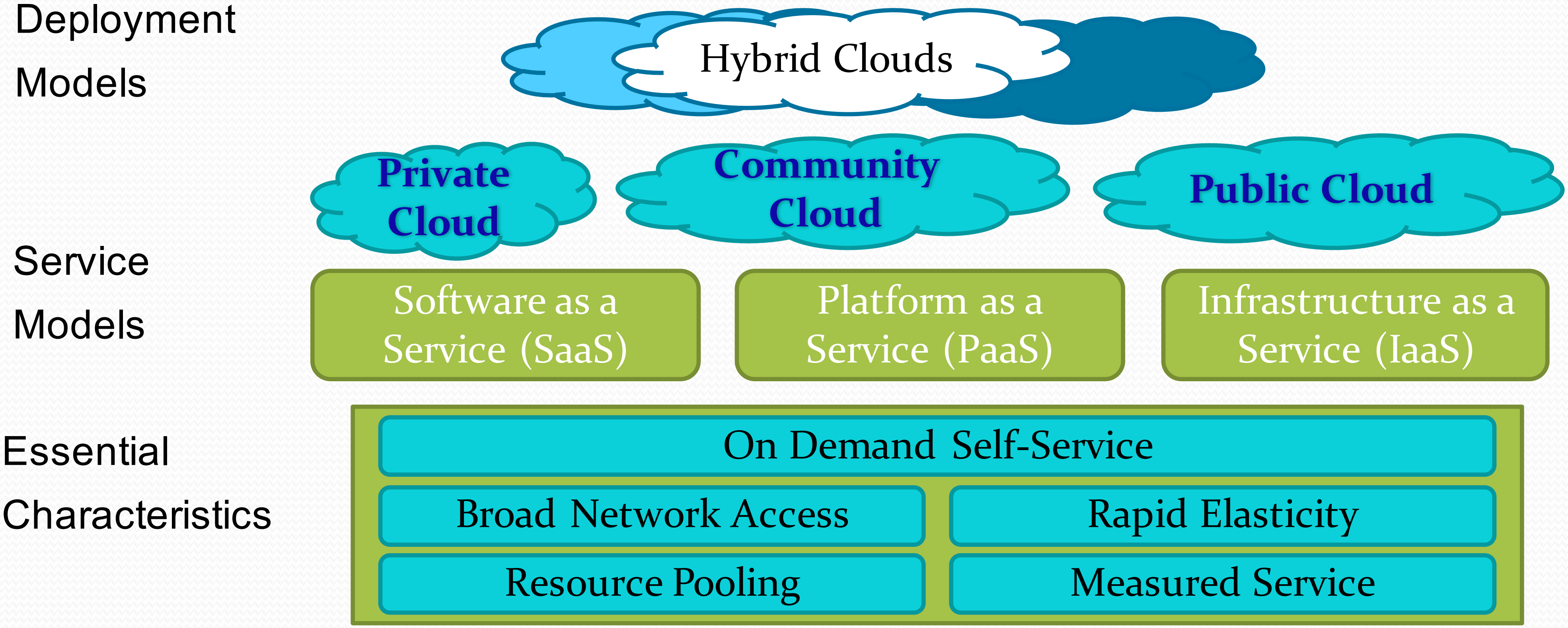
What Is Cloud Computing?

- Wikipedia Definition
  - Cloud computing is a concept of using the Internet to allow people to access technology-enabled services
  - It allows users to consume services without knowledge of control over the technology infrastructure that supports them

- NIST Definition
  - 5 essential characteristics
  - 3 cloud service models
  - 4 cloud deployment models



The NIST Cloud Definition Framework



Deployment Models

Hybrid Clouds

Private Cloud

Community Cloud

Public Cloud

Service Models

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Essential Characteristics

On Demand Self-Service

Broad Network Access

Rapid Elasticity

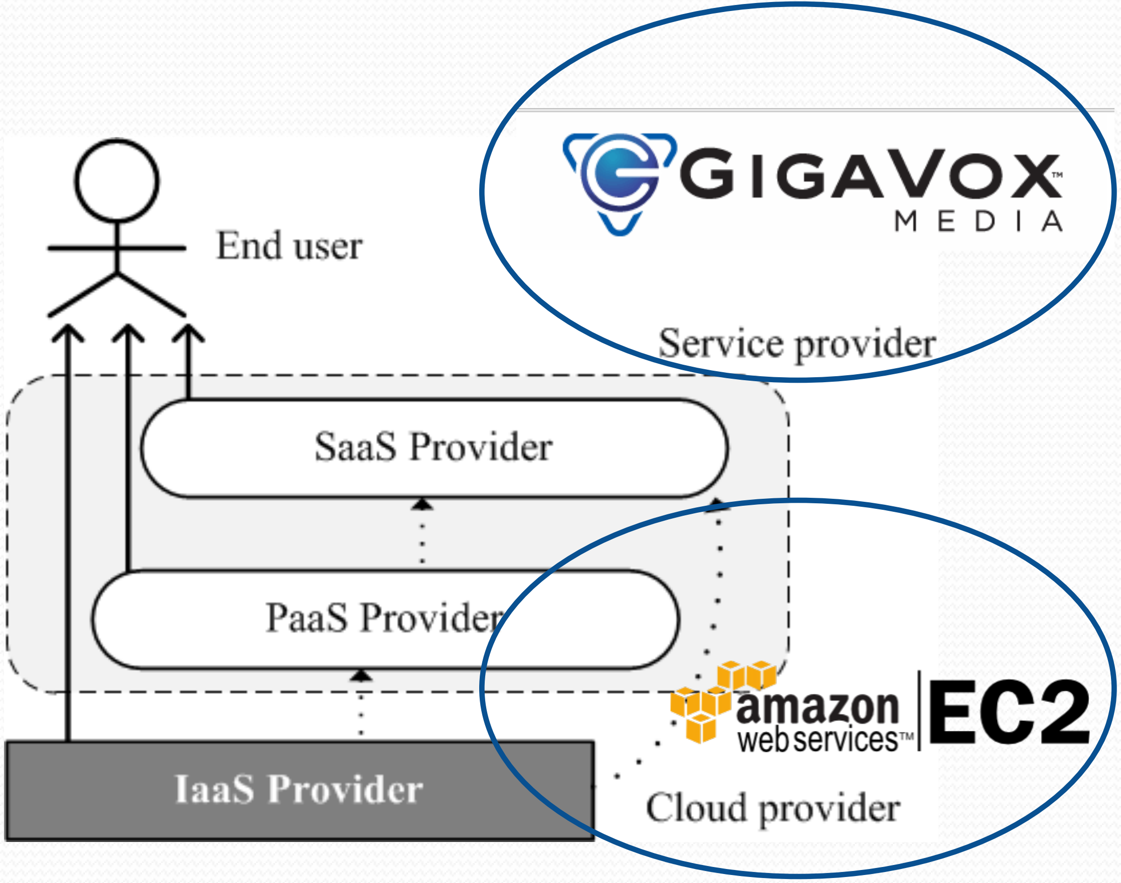
Resource Pooling

Measured Service

NIST Definition Framework

Typical Cloud System Model

- Cloud Service Providers (CSPs)
  - Cloud providers
  - Service providers
- End users



Users and providers in cloud computing

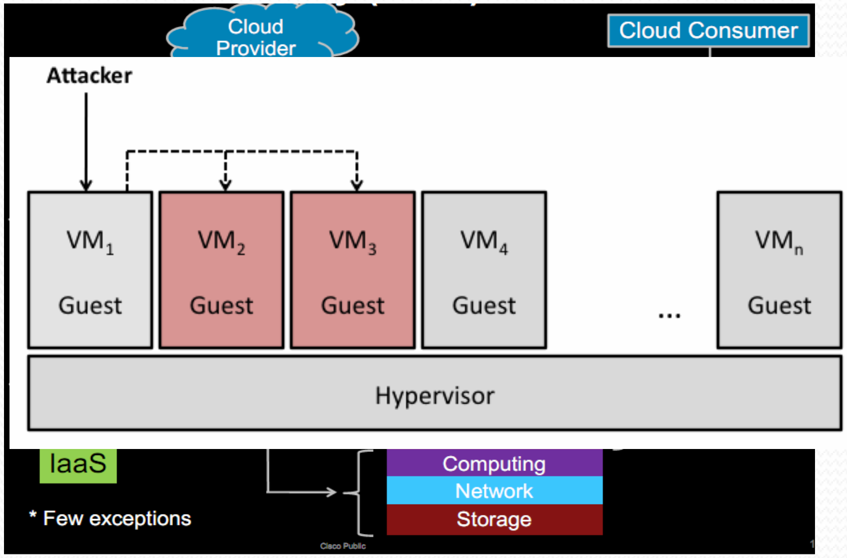
Outline

- Introduction to Cloud Computing
- Security Issues in Cloud Computing
- Data-Centric Security
- User-Controlled Security Mechanism
- Conclusion

Traditional Security Issues

- **Network security**
  - Man-in-the-middle attacks, IP spoofing, ports scanning, packet sniffing
- **Web application vulnerabilities**
  - SQL injection, session riding and hijacking, cross-site scripting
- **Distributed Denial of Services (DDoS) attacks**
- **Virtualization vulnerabilities**
  - Potential software vulnerabilities
- **Access control weakness**
- **Authentication and authorization security**

New Security Challenges



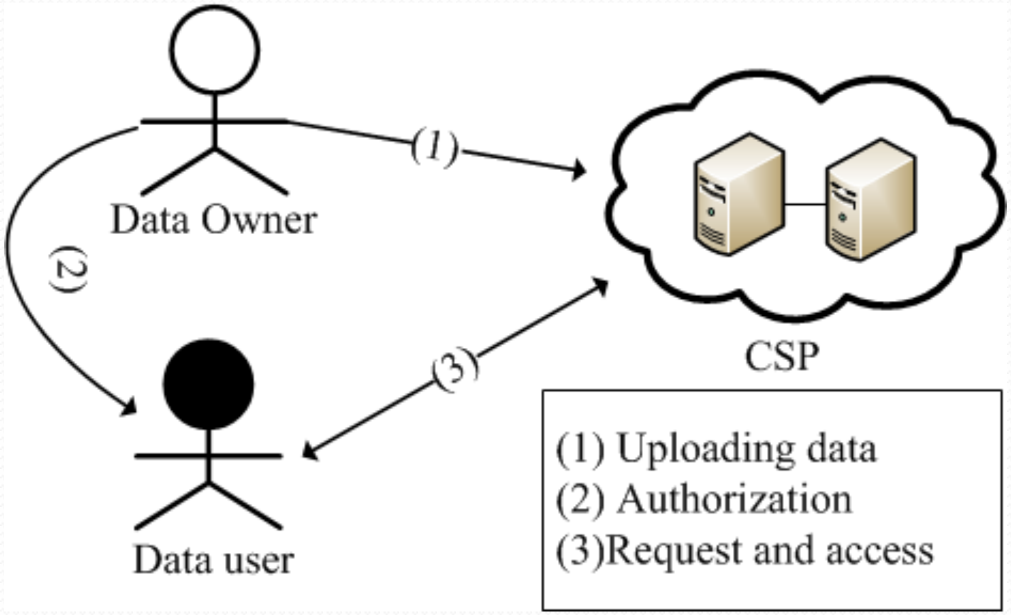
- **Multi-tenancysecurity**
  - *Side-channel attacks, fate of sharing*
  - *Data separation and VMs' isolation*
- **Accountability**
  - *While a data breach happens, it is hard to determine which entities should be blamed for it*
  - *Well-designed SLA, auditability*
- **Innerattacks**
  - *The CSP has the highest privilege to access user data,*
  - *Data encryption*
- **Heterogeneity**
  - *Multi-trusted domains with different security policies*
  - *Standards need to be established*

Outline

- Introduction to Cloud Computing
- Security Issues in Cloud Computing
- Data-Centric Security
- User-Controlled Security Mechanism
- Conclusion

System Model

- **Data owner**
  - Uploads data to clouds maintained by the CSP
- **Data user**
  - Requests data from the CSP after obtaining authorization from the data owner



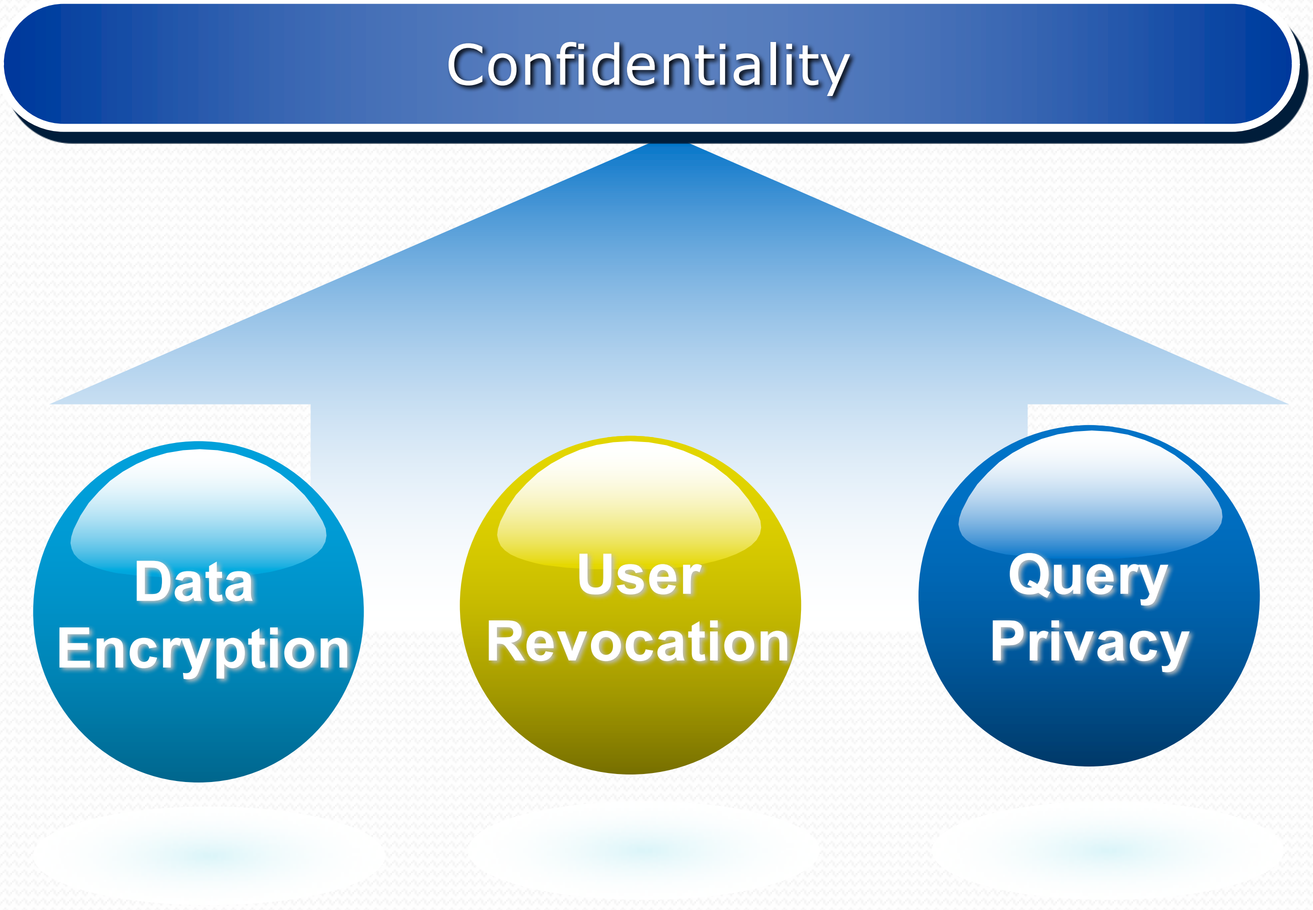
System model in data-centric clouds

Data-centric security mainly refers to ensuring the CIA of data in cloud environments

CIA in Cloud computing

- Confidentiality
  - The prevention of intentional or unintentional unauthorized disclosure of information (Encryption, Access control, Authorization, Authentication)
- Integrity
  - Ensure that unauthorized modifications are not made to data (MAC, DS)
- Availability
  - Ensure the reliable and timely access to data or resources (Multiple data copies)

Confidentiality in Clouds



Confidentiality

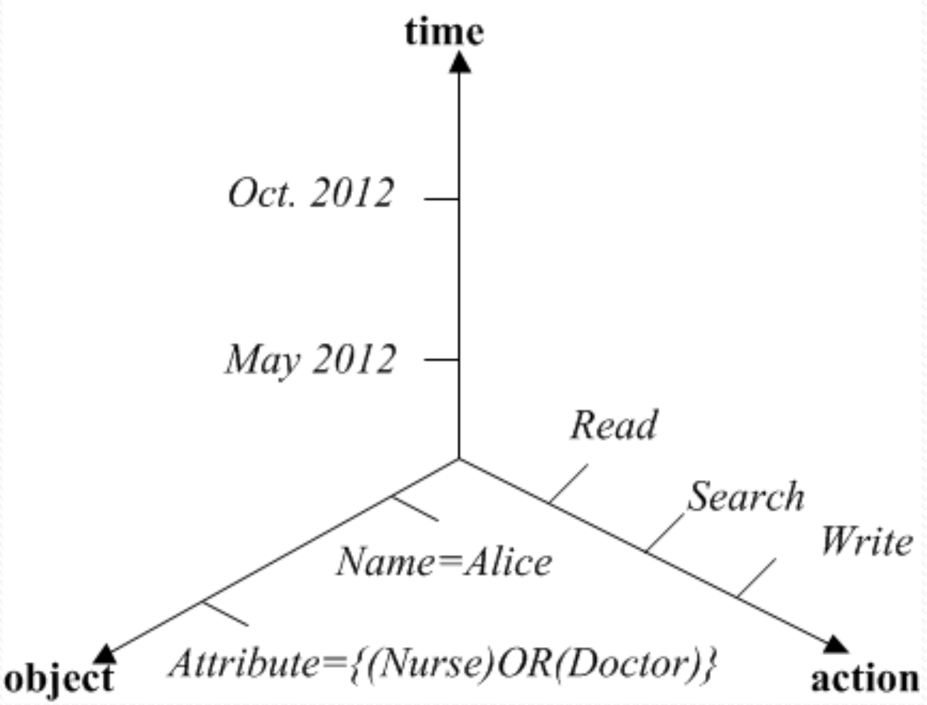
Data Encryption

User Revocation

Query Privacy

Data dimension

- **Object dimension**
  - Describes the data users who have rights to access such data
- **Time dimension**
  - Denotes the length of the access right of the object
- **Action dimension**
  - Describes the *read* right, *write right, and search right of the object*



Data dimensions

Data Encryption

- **Natural way**
  - Adopting cryptographic technique

- **Current solutions**
  - Traditional symmetric/ asymmetric encryption
    - Low cost for encryption and decryption
    - Hard to achieve fine-grained access control
  - Attribute-Based encryption (ABE)
    - Easy to achieve fine-grained access control

User Revocation

- **Naïve solution**
  - The data owner re-encrypts data and distributes new keys to the data user
  - Frequent revocation will make the data owner become a performance bottleneck

- **Proxy Re-encryption (PRE)**
  - The data owner to send re-encryption instruction to the cloud
  - The cloud perform re-encryption based on PRE

Query Privacy

- **Query privacy**
  - Search privacy: Protect what the users are searching for
  - Access privacy: Protect what/which files are returned to the users

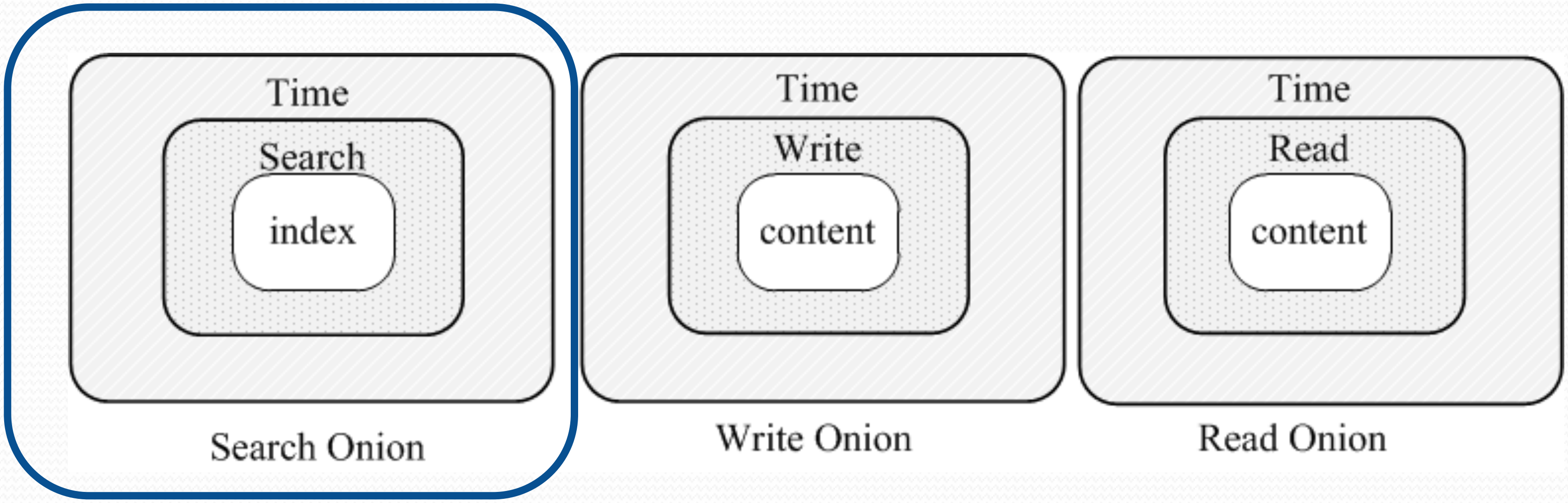
- **Existing solutions**
  - Searchable encryption (SE) can protect search privacy while searching encrypted data

Outline

- Introduction to Cloud Computing
- Security Issues in Cloud Computing
- Data-Centric Security
- User-Controlled Security Mechanism
- Conclusion

Onion Encryption

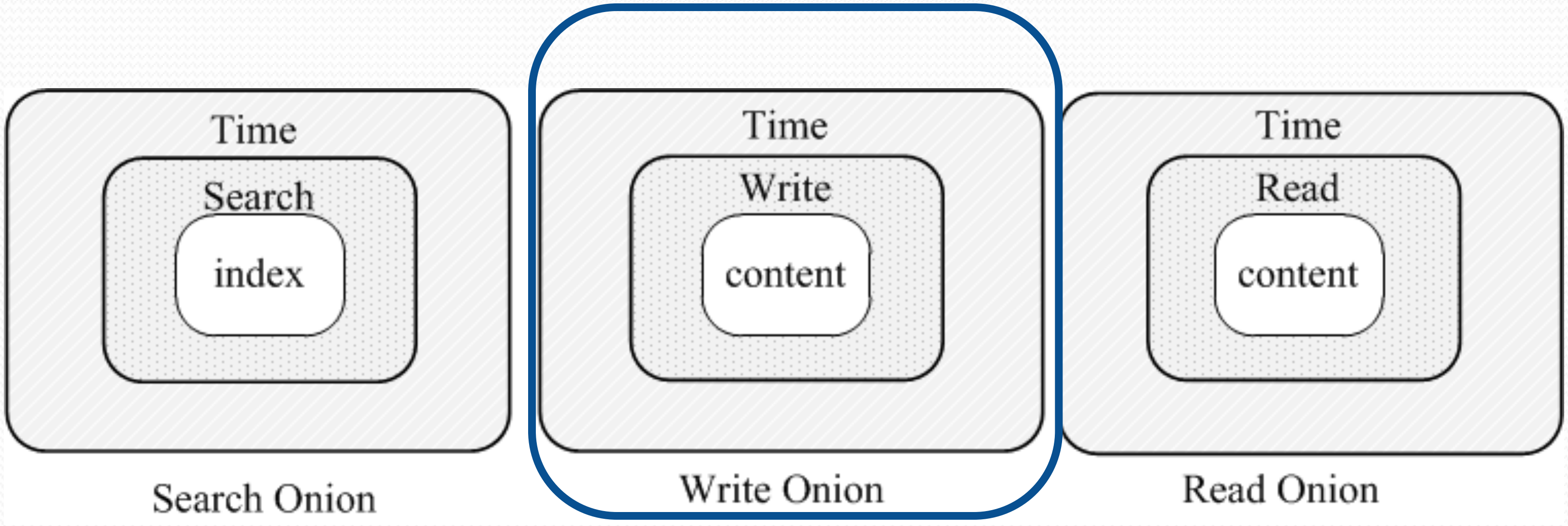
- **Search onion**
  - *Associate each piece of data with an index that includes several keywords describing the data content*
  - *Index is encrypted with the search layer, which can be encapsulated with searchable encryption*



Onion encryption layers

Onion Encryption

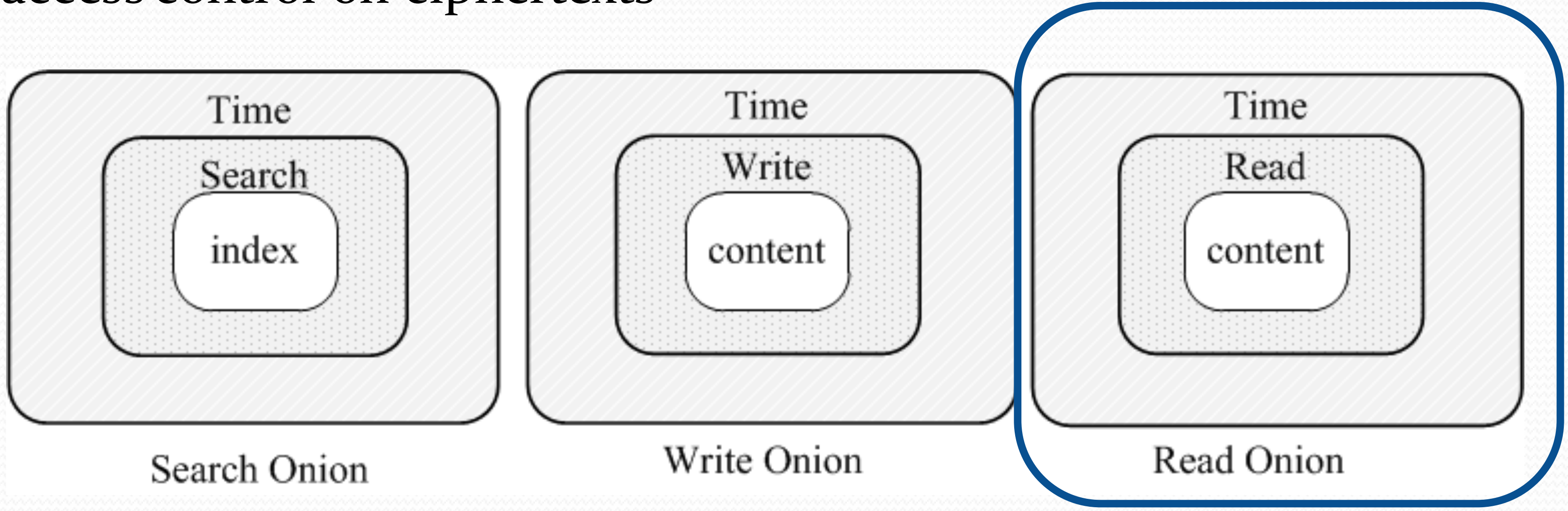
- **Write onion**
  - *The content can be encrypted with homomorphic encryption , where the computations can be performed directly on the ciphertexts without decryption*



Onion encryption layers

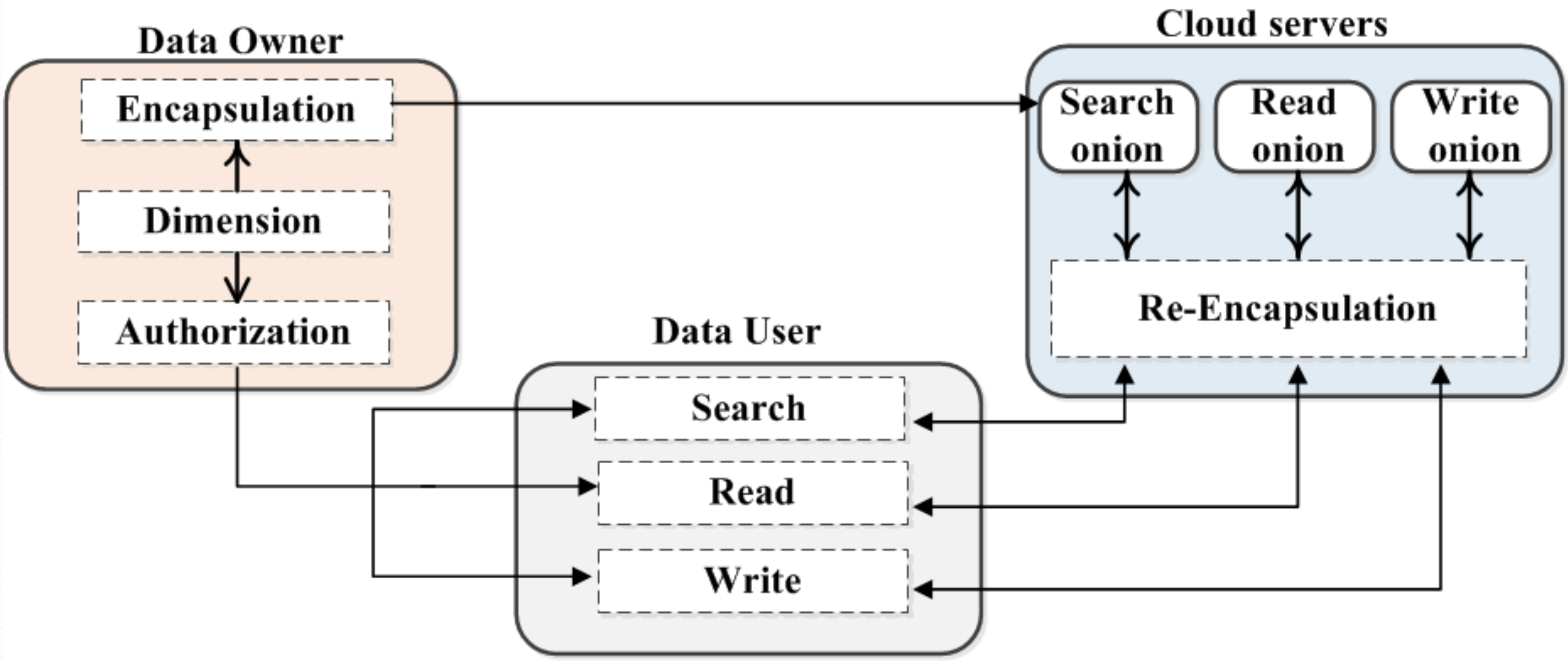
Onion Encryption

- **Read onion**
  - Encrypts data content with a symmetric key, which is in turn encrypted with ABE over a specific access structure
  - Applies proxy re-encryption (PRE) into ABE for ensuring dynamic access control on ciphertexts



Onion encryption layers

The user-controlled security mechanism



The users have the ability to customize their desired security level and mechanism on demand

Conclusion

- We investigate the definition, features of cloud computing
- We discuss the security challenges in cloud computing
- We propose user-controlled security in mechanism to achieve data-centric security in clouds

ANY QUESTIONS?