Forensics-as-a-Service and Models for Forensic Brokerage

Dr. Keyun Ruan
University College Dublin

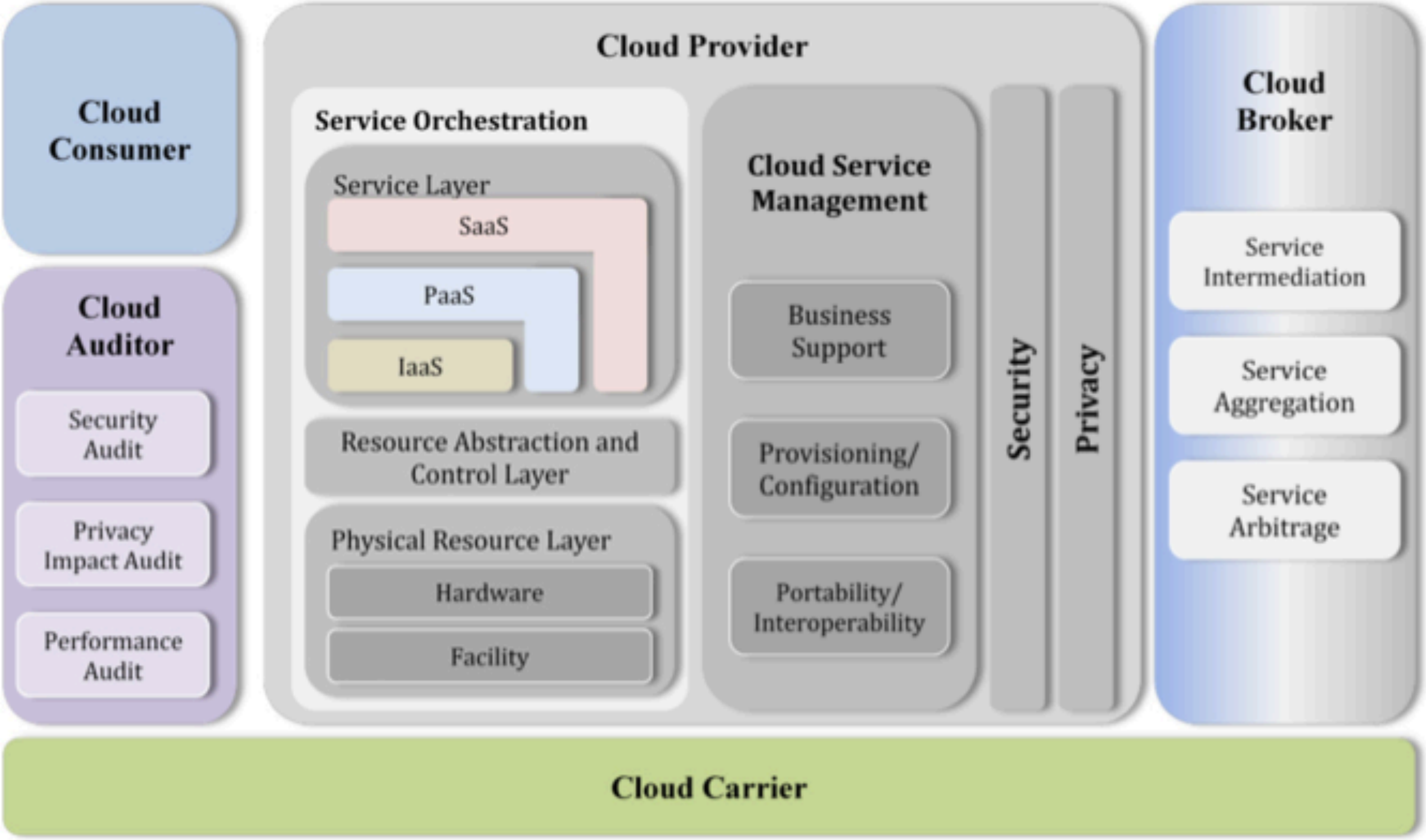
TAFC/IFIP11.11, 6 June 2013 Malaga, Spain

What is Cloud Forensics?

- Law enforcement perspective
- Security perspective
- Traditional digital forensic challenges
- Digital forensics in the cloud ecosystem

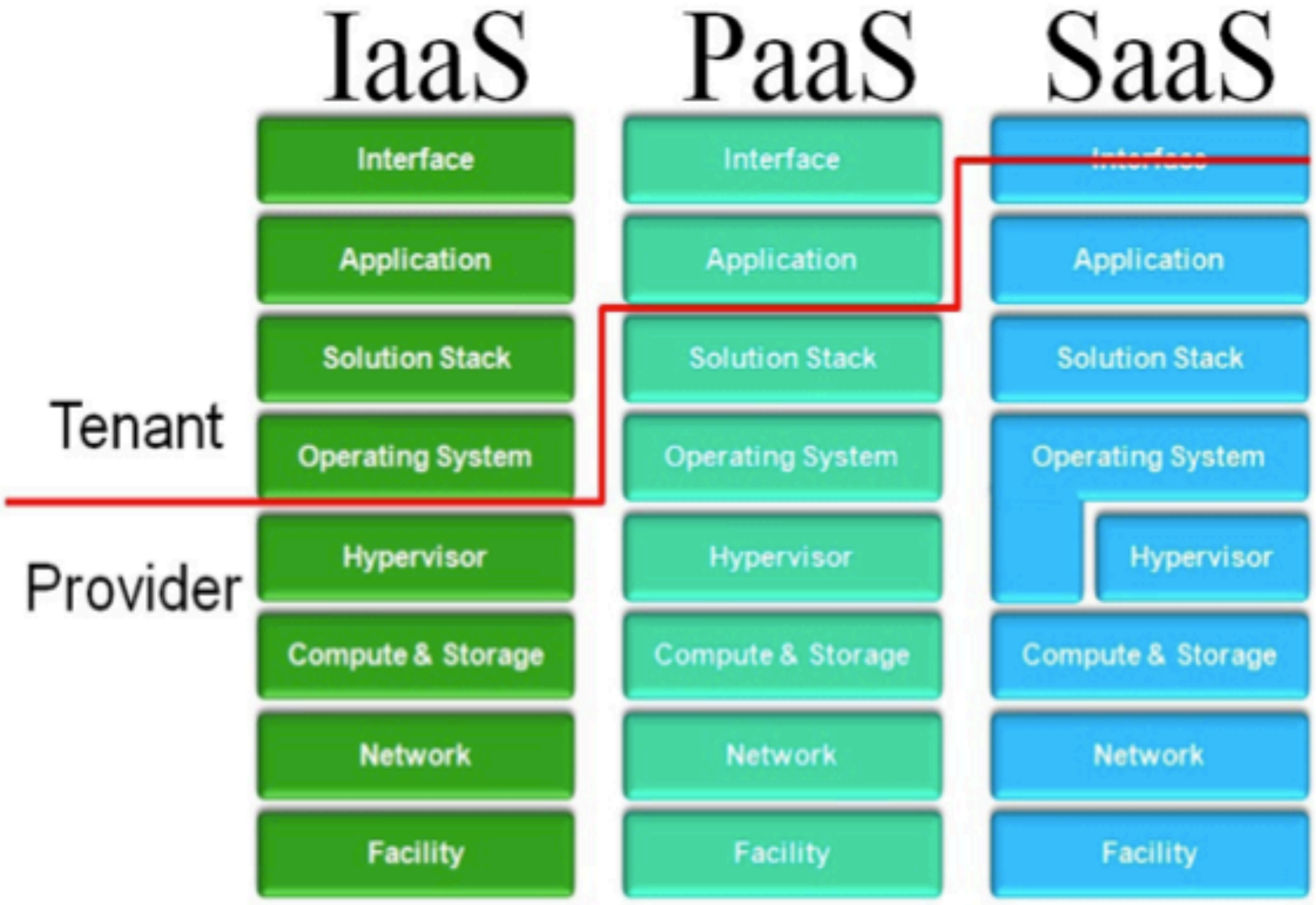
Organizational Challenges

- Split of control
- Segregation of duties
- Chain of dependencies
- Lack of transparency

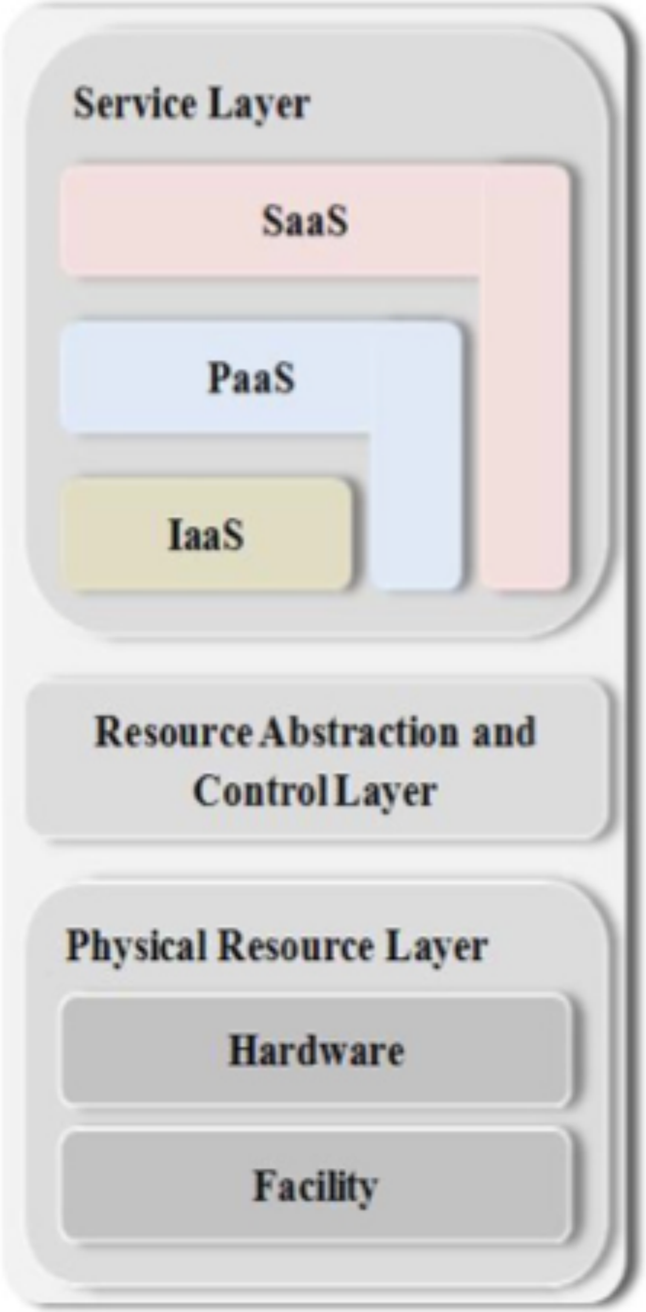


Source: NIST 500-292 Cloud Computing Reference Architecture

Technical Challenges



Source: Brenton, C. (2012) 'Can I Outsource My Security to the Cloud?', SANS blog, 19 Jul 2012



Source: NIST SP 500-292

Technical Challenges

- Hybrid forensic acquisition
- Evidence segregation
- Instance isolation
- Time synchronization
- Data integrity

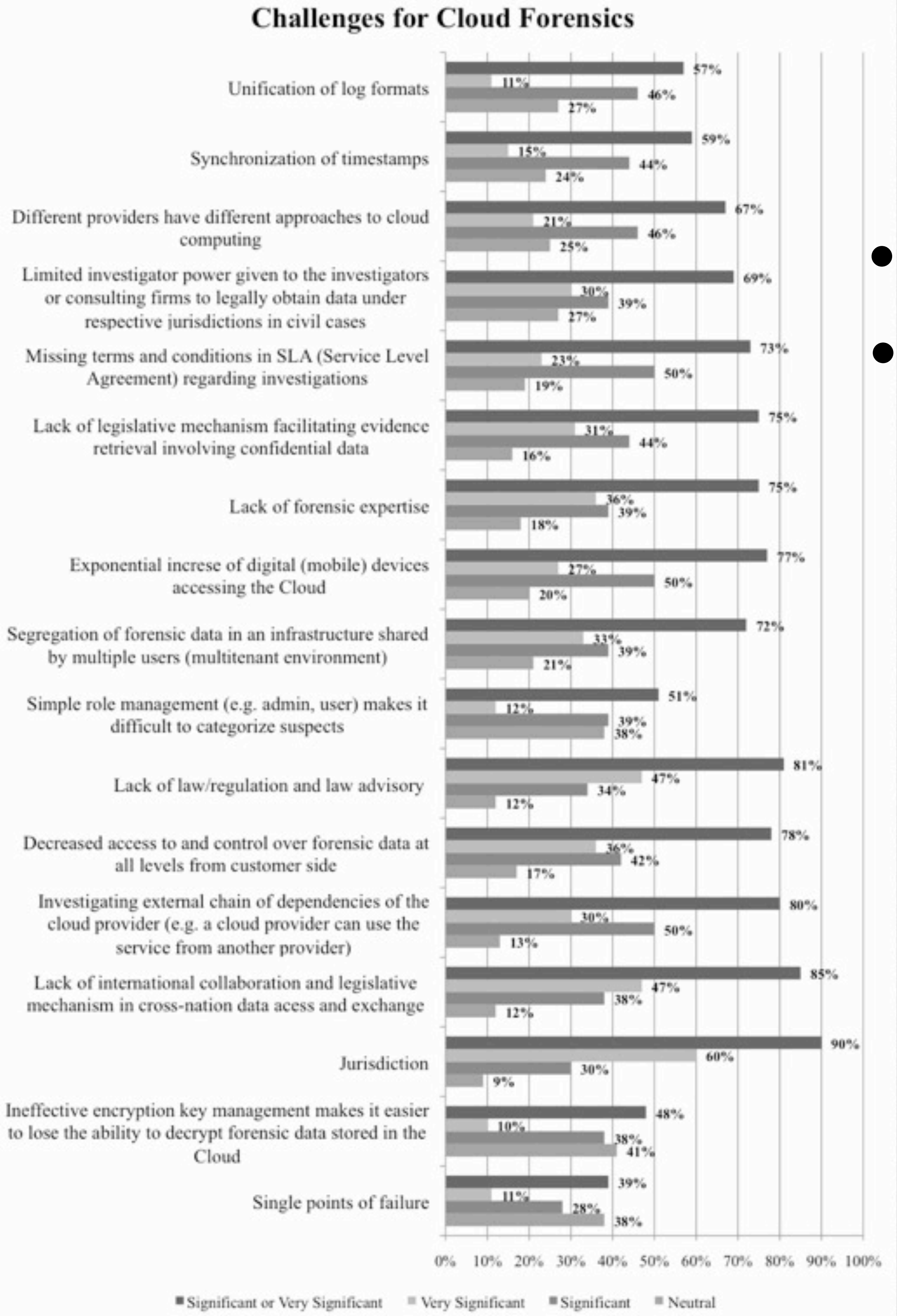
- Identity and anonymity
- E-discovery
- Proliferation of endpoints
- Encryption
- Interoperability
- ...

NIST Cloud Computing Forensic Science Working Group: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudForensics

Legal Challenges

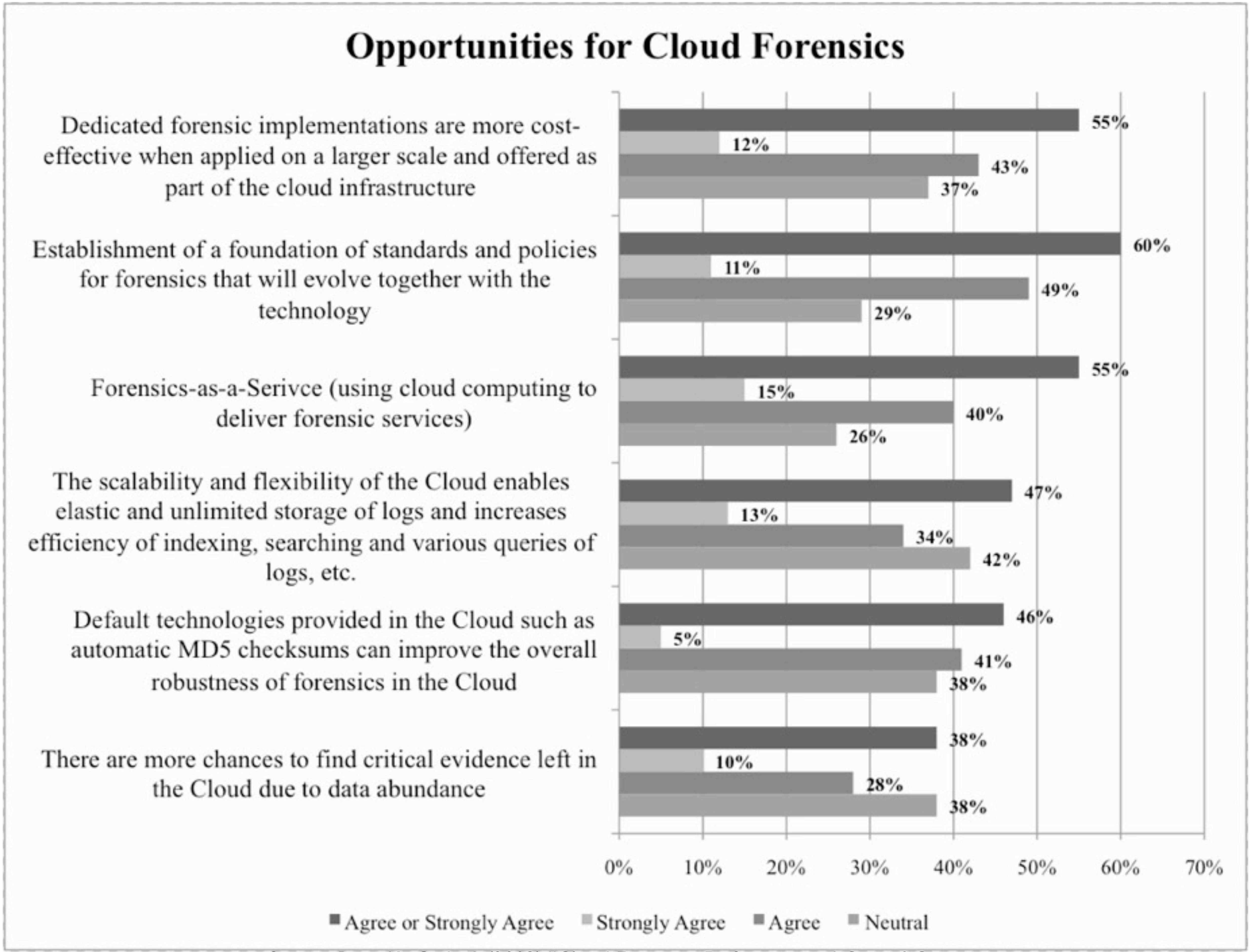
- Multi Jurisdiction
- Multi Tenancy
- Data Ownership
- Privacy
- Service Level Agreement

Survey Results



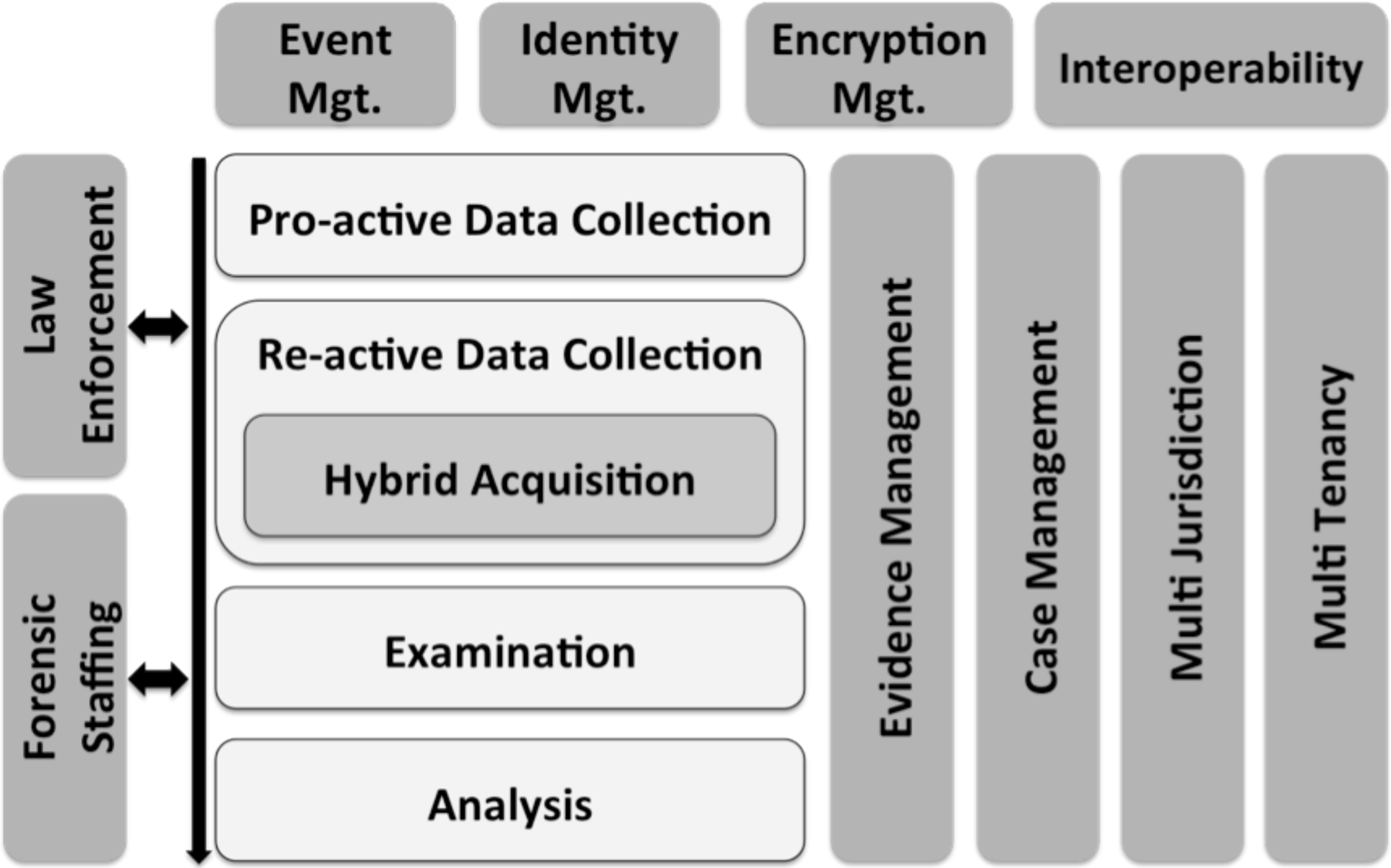
- 257 respondents
- *Proposed definition: "Cloud Forensics is the application of digital forensic science in cloud computing environments. Technically, it consists of a hybrid forensic approach (e.g., remote, virtual, network, live, large-scale, thin-client, thick-client) towards the generation of digital evidence. Organizationally it involves interactions among cloud actors (i.e., cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor) for the purpose of facilitating both internal and external investigations. Legally it often implies multi-jurisdictional and multi-tenant situations.*

Source: Ruan K., Cathy J. (2013) "Cloud Forensics Definitions and Critical Criteria for Cloud Forensic Capability:an Overview of Survey Results", Digital Investigation, Elsevier

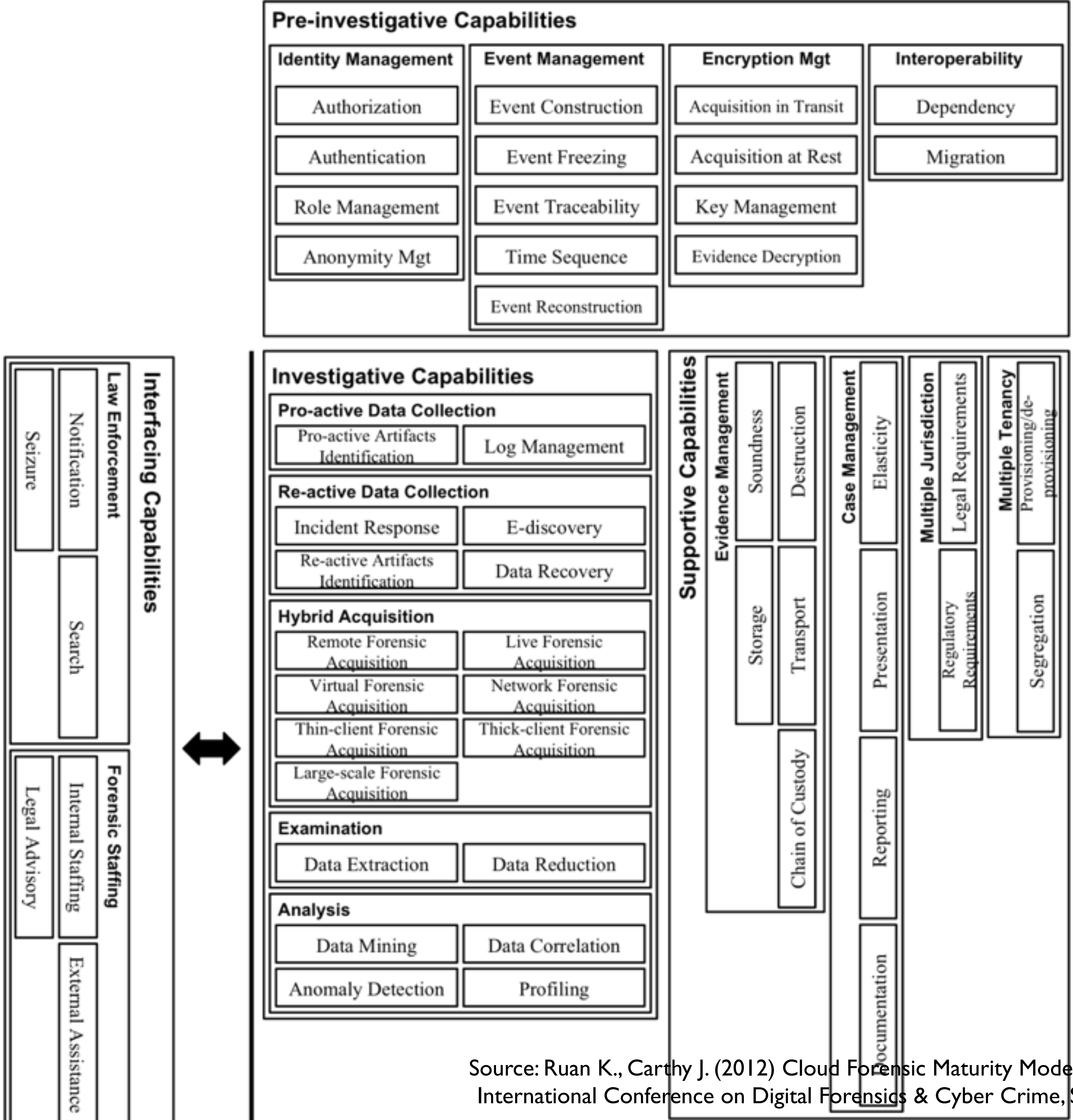


Source: Ruan K., Cathy J. (2013) "Cloud Forensics Definitions and Critical Criteria for Cloud Forensic Capability:an Overview of Survey Results", Digital Investigation, Elsevier

Cloud Forensic Investigative Architecture



Source: Ruan K., Carthy J. (2012) Cloud Forensic Maturity Model, Proceedings of the 4th International Conference on Digital Forensics & Cyber Crime, Springer Lecture Notes



Pre-investigative Capabilities

Identity Management
- Authorization
- Authentication
- Role Management
- Anonymity Mgt

Event Management
- Event Construction
- Event Freezing
- Event Traceability
- Time Sequence
- Event Reconstruction

Encryption Mgt
- Acquisition in Transit
- Acquisition at Rest
- Key Management
- Evidence Decryption

Interoperability
- Dependency
- Migration

Interfacing Capabilities

Law Enforcement
- Notification
- Seizure
- Search

Forensic Staffing
- Internal Staffing
- Legal Advisory
- External Assistance

Investigative Capabilities

Pro-active Data Collection
- Pro-active Artifacts Identification
- Log Management

Re-active Data Collection
- Incident Response
- E-discovery
- Re-active Artifacts Identification
- Data Recovery

Hybrid Acquisition
- Remote Forensic Acquisition
- Live Forensic Acquisition
- Virtual Forensic Acquisition
- Network Forensic Acquisition
- Thin-client Forensic Acquisition
- Thick-client Forensic Acquisition
- Large-scale Forensic Acquisition

Examination
- Data Extraction
- Data Reduction

Analysis
- Data Mining
- Data Correlation
- Anomaly Detection
- Profiling

Supportive Capabilities

Evidence Management
- Soundness
- Destruction
- Storage
- Transport
- Chain of Custody

Case Management
- Elasticity
- Presentation
- Reporting
- Documentation

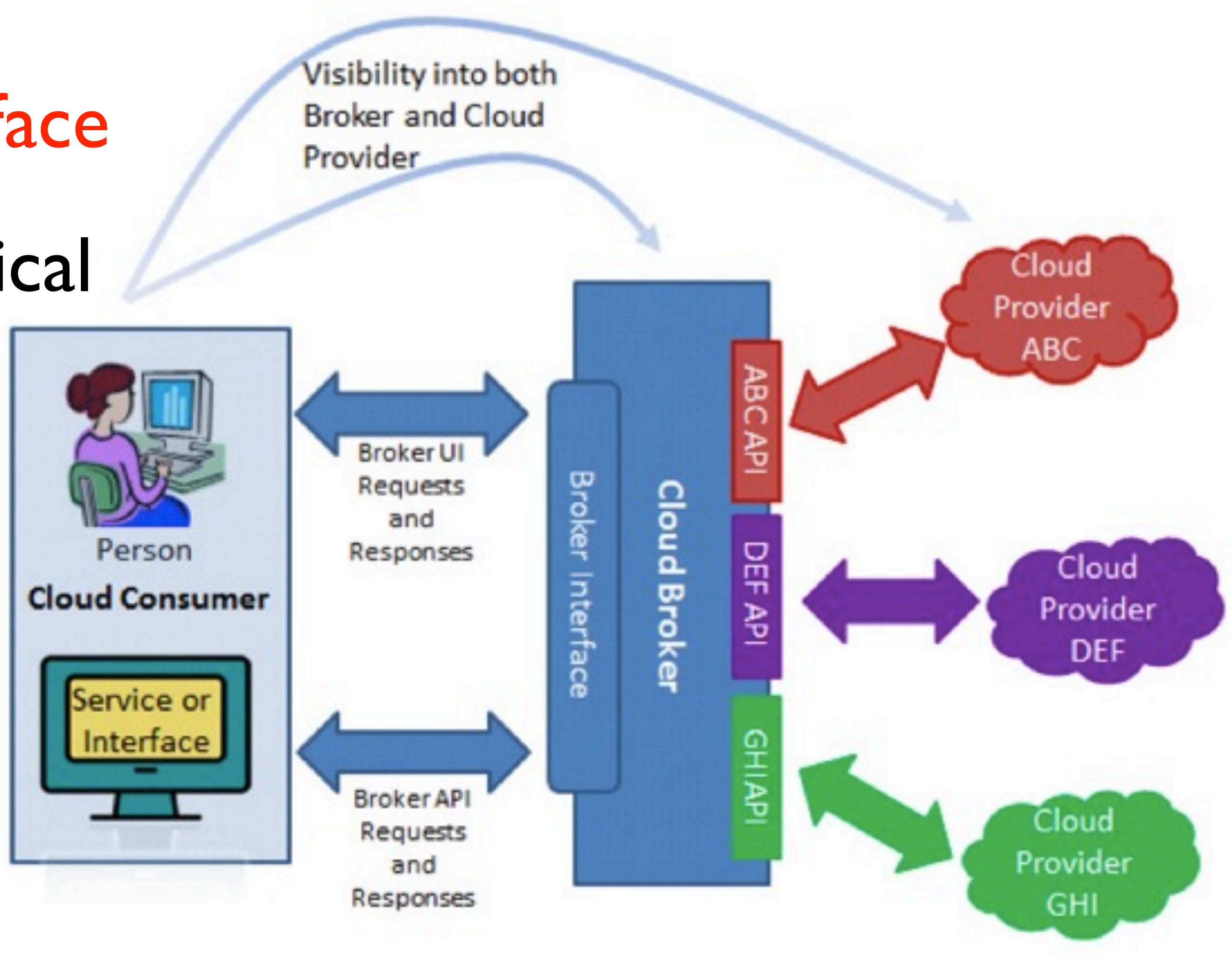
Multiple Jurisdiction
- Legal Requirements
- Regulatory Requirements

Multiple Tenancy
- Provisioning/de-provisioning
- Segregation

Source: Ruan K., Carthy J. (2012) Cloud Forensic Maturity Model, Proceedings of the 4th International Conference on Digital Forensics & Cyber Crime, Springer Lecture Notes

FaaS and Cloud Brokerage

- Single consistent interface
- Business broker, technical broker, or both
- Aggregation
- Arbitrage
- Intermediation



Source: NIST SP 500-292

Models for Cloud Forensic Brokerage

Key Features:

- Elasticity
- FaaS
- Big data/analytics
- Standard Interface

- Broker for Investigative Capability
- Broker for Investigative Process
- Broker for Investigative Toolkit

Key Takeaways

- Cloud forensics poses significant challenges in organizational, technical and legal dimensions
- Definition of cloud forensics
- There are opportunities to be leveraged for cloud forensics including FaaS and standardization acceleration
- Cloud Forensic Investigative Architecture
- Models for cloud forensic brokerage

My Book

- Cybercrime and Cloud Forensics: Applications for Investigation Processes, IGI Global, December 2012: http://www.igi-global.com/book/cybercrime-cloud-forensics/69206

Questions?

Thank you!

- @ruankeyun
- keyun.ruan@ucd.ie
- www.cloudforensicsresearch.org