Cloud Forensics: an Overview

Keyun Ruan

Center for Cyber Crime Investigation
University College Dublin

Cloud Futures 2011, Microsoft Research Redmond, June 3, 2011

Co-authors

- Mark Crosbie, IBM Ireland
- Joshua James, University College Dublin
- Ibrahim Baggili (PhD), Zayed University, UAE
- Prof. Joe Carthy, University College Dublin
- Prof. Tahar Kechadi, University College Dublin

Funding

- The Irish Research Council for Science, Engineering & Technology (IRCSET)
- The European Aeronautic Defence and Space Company N.V. (EADS)

DIGITAL INVESTIGATION IN THE CLOUD

- Global interconnection, openness and interoperability
- Safe havens
- Modern consumer, business, political, scientific, and educational activities will be powered by cloud computing
- Cybercrime (105 billion) > Drug dealing
- Law enforcement not catching up
- “To avoid breaches, the good guys have to succeed 100% of the time. The bad guys only have to succeed once”

"States must identify and prosecute cyber criminals, to ensure laws and practices deny criminals safe havens, and cooperate with international criminal investigations in a timely manner."

International Strategy for Cyberspace, May 2011

What happened and what is happening in the Cloud?

CLOUD FORENSICS IS MULTI-DIMENSIONAL

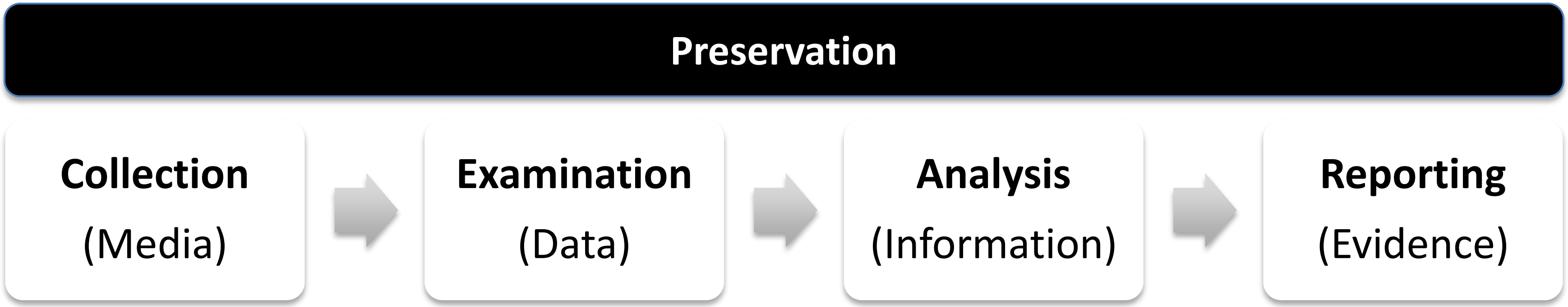
Technical Dimension

Chain of custody
Admissibility

Soundness
Transport

Storage
Destroy

Case management



Preservation

Collection
(Media)

Examination
(Data)

Analysis
(Information)

Reporting
(Evidence)

Pro-active
Client-side
Provider-side
Data sources
Mobile endpoints
Physical locations
Sampling
Time sync
…

Evidence segregation
Traceability
Filtering
Pattern matching
Data reduction
…

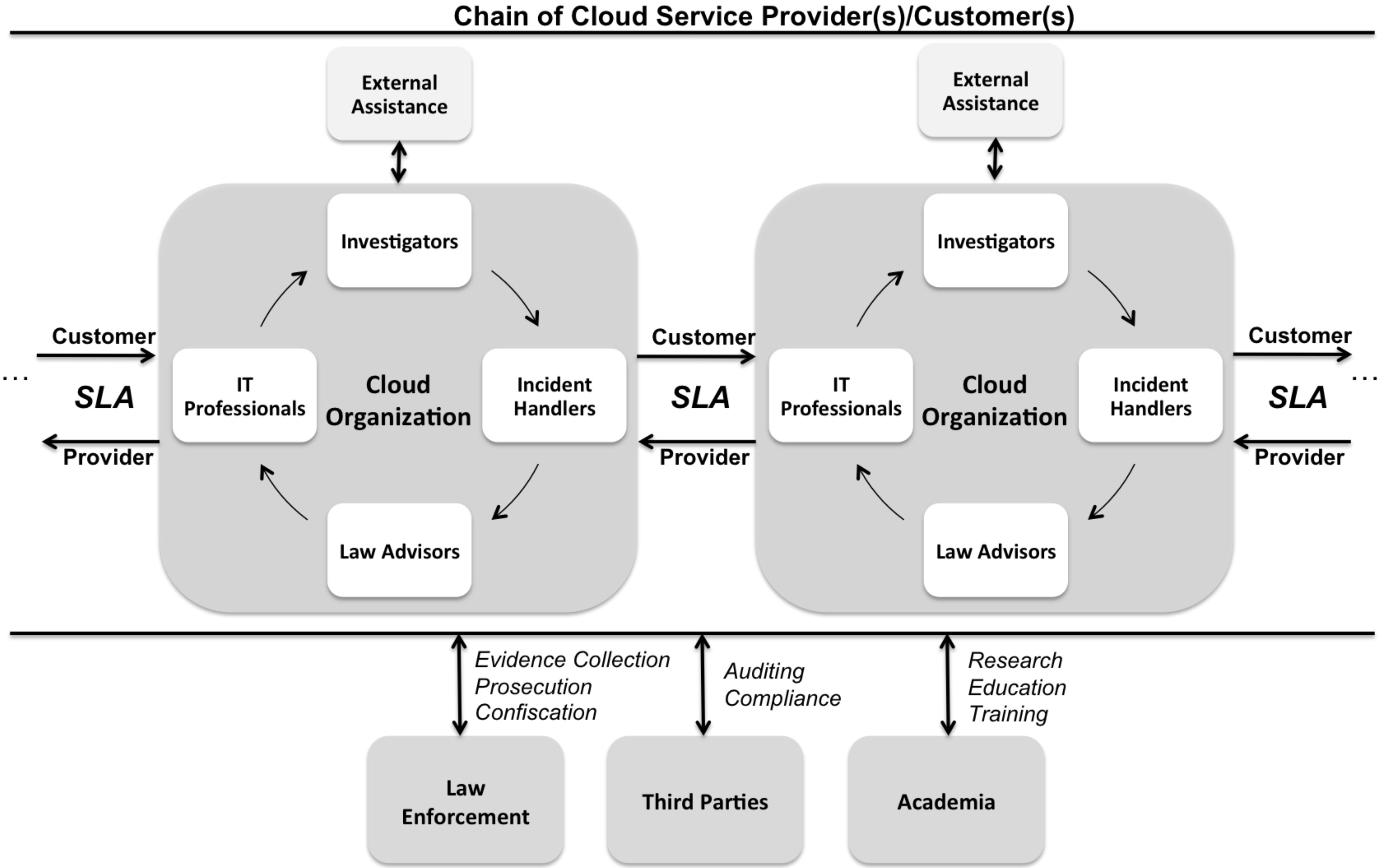
Data mining
Reconstruction
Time sequence
…

Documentation
Presentation
Expert testimony

5 main areas of focus

- Forensic data collection
- Elastic, static & live forensic toolkits
- Evidence segregation
- Investigative tools in virtualized environments
- Pro-active preparations

Organizational Dimension



3 main areas of focus

- Segregation of duties
- Collaboration
- Policy

Legal Dimension

- Multi-jurisdiction
- Multi-tenancy
- Multi-ownership
- Service Level Agreement

WHAT DO EXPERTS SAY?

Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability

- Launched 13th Feb 2011
- **156** responses up to 23rd Mar 2011
- 192 responses up to now

50%: CLOUD MAKES FORENSICS HARDER

- Loss of data control
- No access to physical infrastructure
- Legal issues of multi-jurisdiction
- Multi-tenancy and multi-ownership
- Lack of tools for larger-scale distributed and virtualized systems
- No standard interfaces
- No provider cooperation
- Difficulties in producing forensically sound and admissible evidence in court

- More computing resources and processing power with reduced cost
- Rapidly scalable auditing, reporting, and testing analysis can be used for larger datasets and distributed applications
- Forensic implementations and activities can be centrally administered and managed
- Investigations can be provided as a service by the CSP

42%: CLOUD MAKES FORENSICS EASIER

Technical Dimension **84%**

Legal Dimension **84%**

Organizational Dimension 75%

TOP 5 CHALLENGES

Jurisdiction	**90.14%**
Investigating external chain of dependencies of the cloud provider	86.12%
Lack of international collaboration and legislative mechanism in cross-nation data access and exchange	84.72%
Lack of law/regulation and law advisory	82.94%
Decreased access to and control over forensic data at all levels from customer side	79.17%

TOP 3 OPPORTUNITIES

Establishment of a foundation of standards and policies	**59.72%**
Forensics-as-a-Cloud-Service	57.14%
Cost-effective forensic implementations as part of cloud infrastructure	53.52%

TOP 3 MOST VALUABLE RESEARCH DIRECTIONS

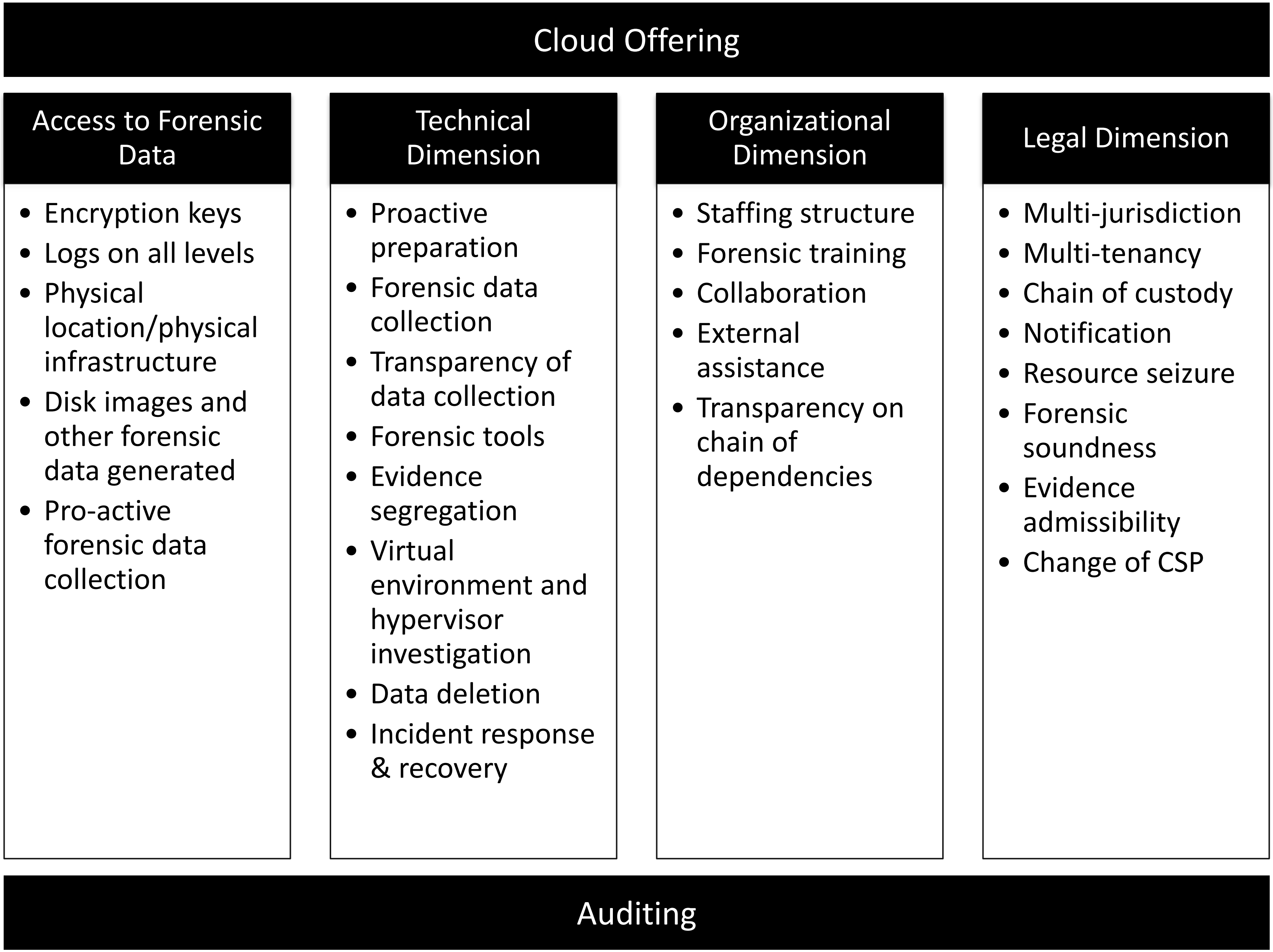
Designing forensic architecture for the Cloud	**88.57%**
Extending current investigative tools into the Cloud	82.86%
Law	82.2%

TOP 5 MOST NEEDED TOOLS AND PROCEDURES

A procedure and a set of toolkits to..

preserve the soundness of digital evidence	**89.55%**
retrieve forensic data involving confidential data under jurisdiction(s) and agreement(s) under which services are operating	87.87%
investigate external chain of dependencies	85.07%
preserve volatile data	83.58%
Proactively collect forensic data	83.58%

SERVICE LEVEL AGREEMENT



Cloud Offering

Access to Forensic Data

- Encryption keys
- Logs on all levels
- Physical location/physical infrastructure
- Disk images and other forensic data generated
- Pro-active forensic data collection

Technical Dimension

- Proactive preparation
- Forensic data collection
- Transparency of data collection
- Forensic tools
- Evidence segregation
- Virtual environment and hypervisor investigation
- Data deletion
- Incident response & recovery

Organizational Dimension

- Staffing structure
- Forensic training
- Collaboration
- External assistance
- Transparency on chain of dependencies

Legal Dimension

- Multi-jurisdiction
- Multi-tenancy
- Chain of custody
- Notification
- Resource seizure
- Forensic soundness
- Evidence admissibility
- Change of CSP

Auditing

CLOUD FORENSICS CAPABILITY MODEL

Initiatives

COLLECTIVE KNOWLEDGE

- Cybercrime and Cloud Forensics: Applications for Investigative Processes. Vol. 1 Vol. 2
- Cloud Forensics Network
- e-Journal of Cloud Forensics Research, UCD CCI

CASE STUDIES

TOOL DEVELOPMENT

BENCHMARK PROJECT

STANDARD & SLA

MY DISSERTATION

Thank You!

Q&A

keyun.ruan@ucd.ie