Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results

Keyun Ruan, Joe Carthy, Tahar Kechadi, Ibrahim Baggili

Digital Investigation 10, No.1, pp 34-43, 2013

Subject : Digital Forensics

Presenter : Byoungjin Seok

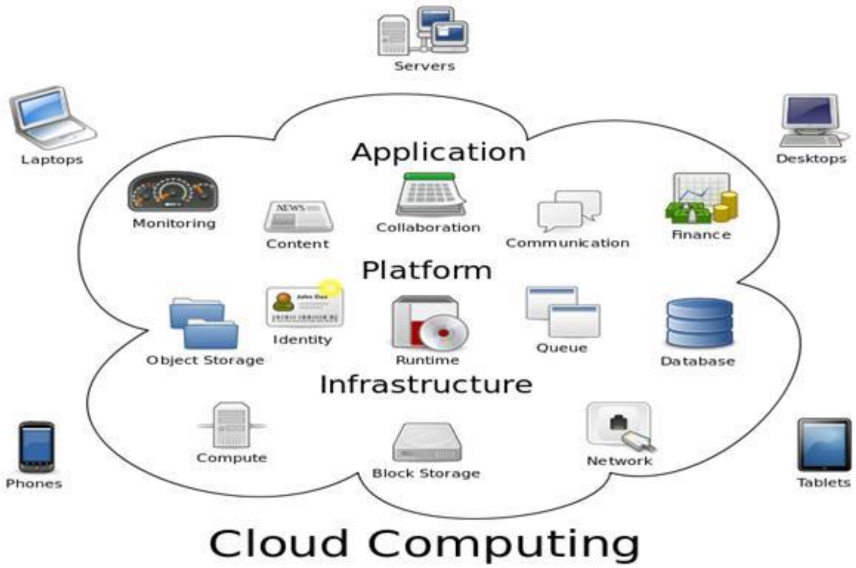
Date : 2017-09-11

Contents

- Cloud computing
- Cloud Forensics
- Survey results

Cloud computing

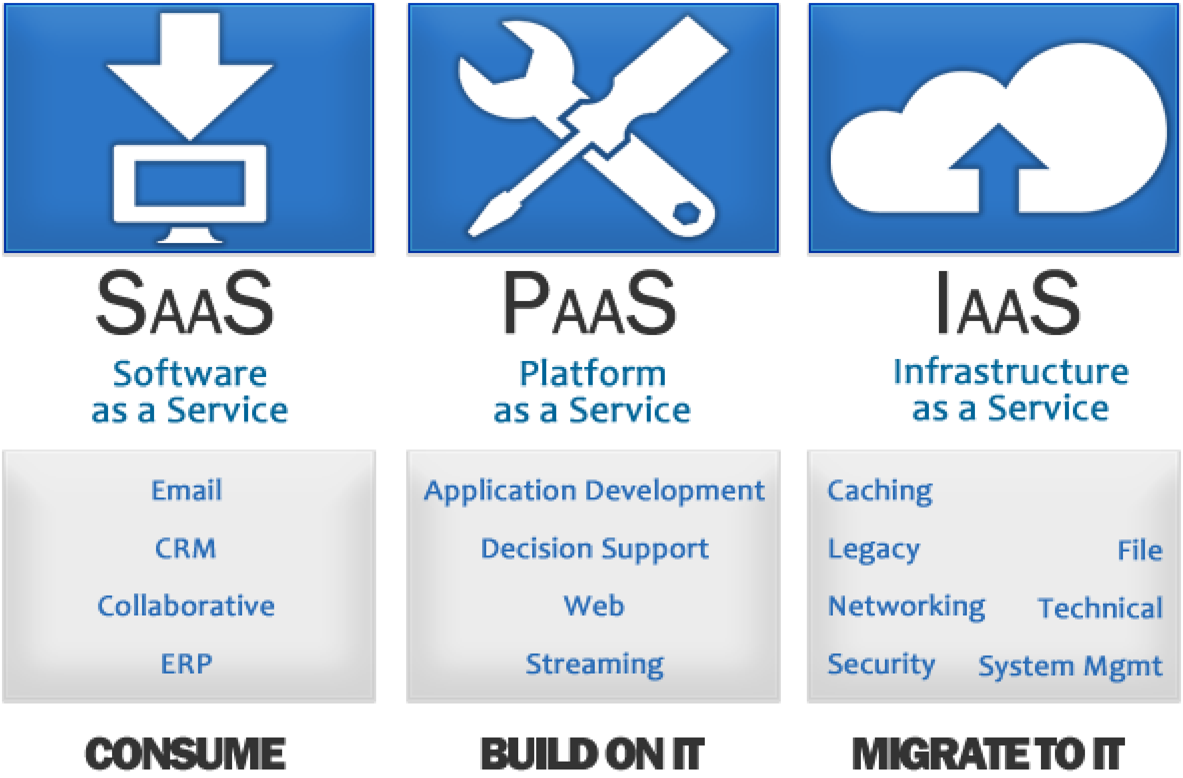
Cloud computing



- Essential Characteristics(NIST SP 800-145)
  - *On-demand self-service* : A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
  - *Broad network access* : Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
  - *Resource pooling* : The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
  - *Rapid elasticity* : Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
  - *Measured service* : Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Cloud computing

- Service models



SaaS

Software as a Service

Email

CRM

Collaborative

ERP

CONSUME

PaaS

Platform as a Service

Application Development

Decision Support

Web

Streaming

BUILD ON IT

IaaS

Infrastructure as a Service

Caching

Legacy

File

Networking

Technical

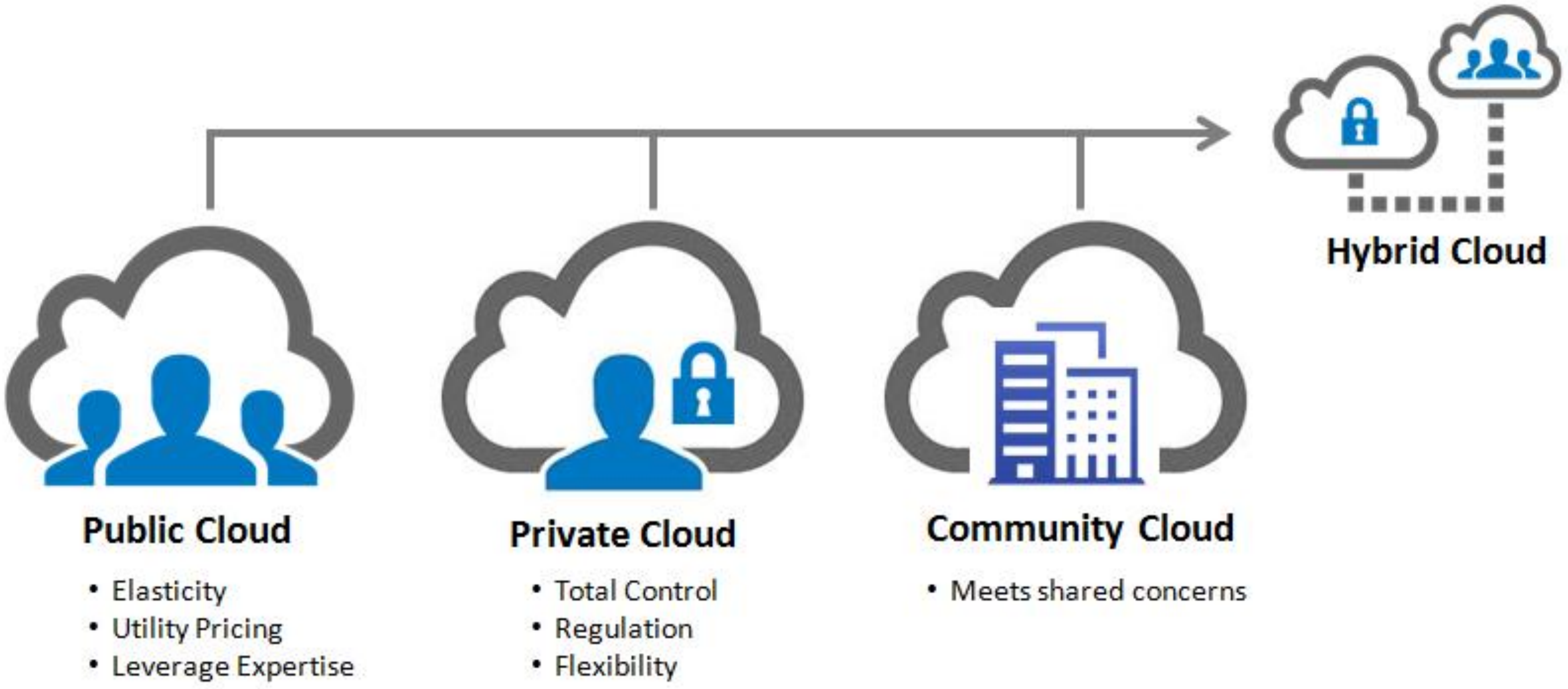
Security

System Mgmt

MIGRATE TO IT

Cloud computing

- Deployment models



Public Cloud

- Elasticity
- Utility Pricing
- Leverage Expertise

Private Cloud

- Total Control
- Regulation
- Flexibility

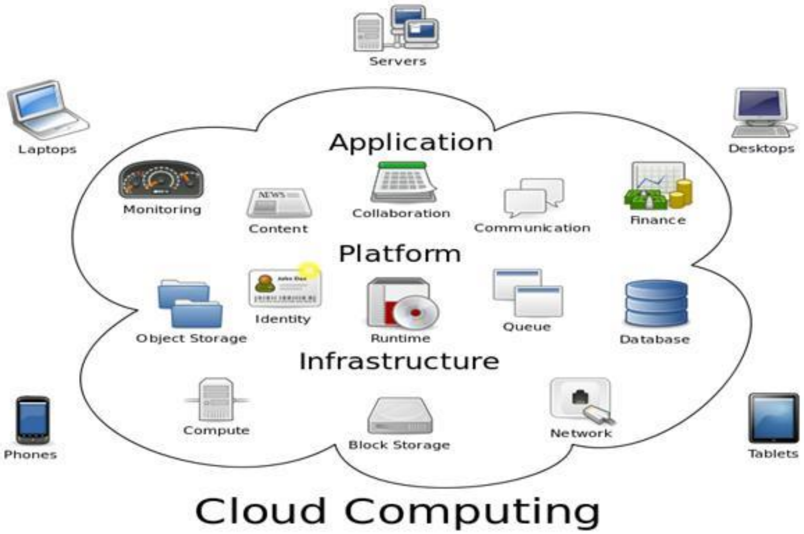
Community Cloud

- Meets shared concerns

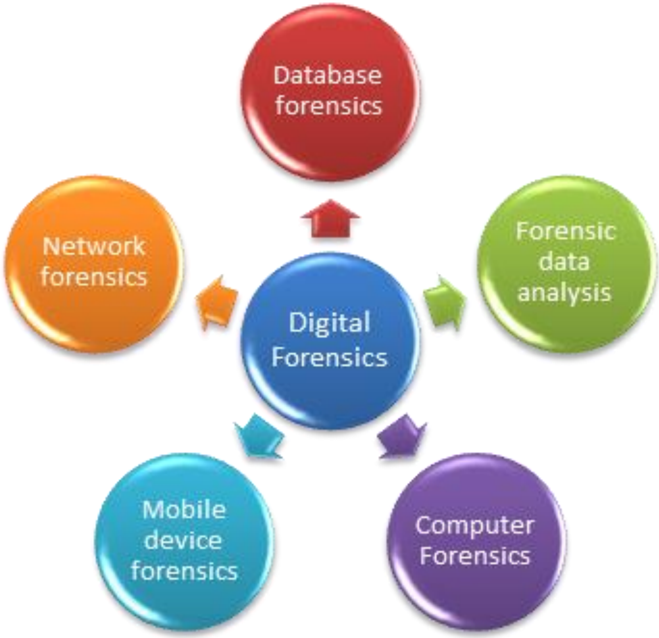
Hybrid Cloud

Cloud Forensics

Cloud Forensics



+



Survey results

List of survey

- Definition of cloud computing
- Cloud computing as a trend
- Cloud forensics definition
- Significance of cloud forensics
- Impact of cloud computing on digital forensics
- Cloud forensics dimensions
- Cloud forensics usage
- Challenges
- Opportunities
- Research directions
- Parties to be assessed for cloud forensic capability
- Guideline, agreement, policy, and staffing importance

Participants

- The survey received 156 responses by March 2011, and up to 1 January 2012, received 257 responses.
- Age(216 participants) :
  - 19~24 years old : 7%
  - 25~30 years old : 15%
  - 31~40 years old : 34%
  - Above 40 years old : 37%
- Male(198 participants) :
  - Male : 85%
  - Female : 15%
- Level of education(202 participants) :
  - Bachelor(or Diploma) degrees : 32%
  - Master degrees : 41%
  - Doctoral degrees : 19%
- Familiarity to digital forensic tools(25 participants) :
  - Very familiar or familiar : 76%
- **Participants are experienced, well-educated, and relatively gave good knowledge as well as sufficient practical experience in the field of digital forensics.**

Definition of cloud computing

- NIST definition of cloud computing version 15

  "Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."(Mell and Grance, 2010)

- The Gartner definition

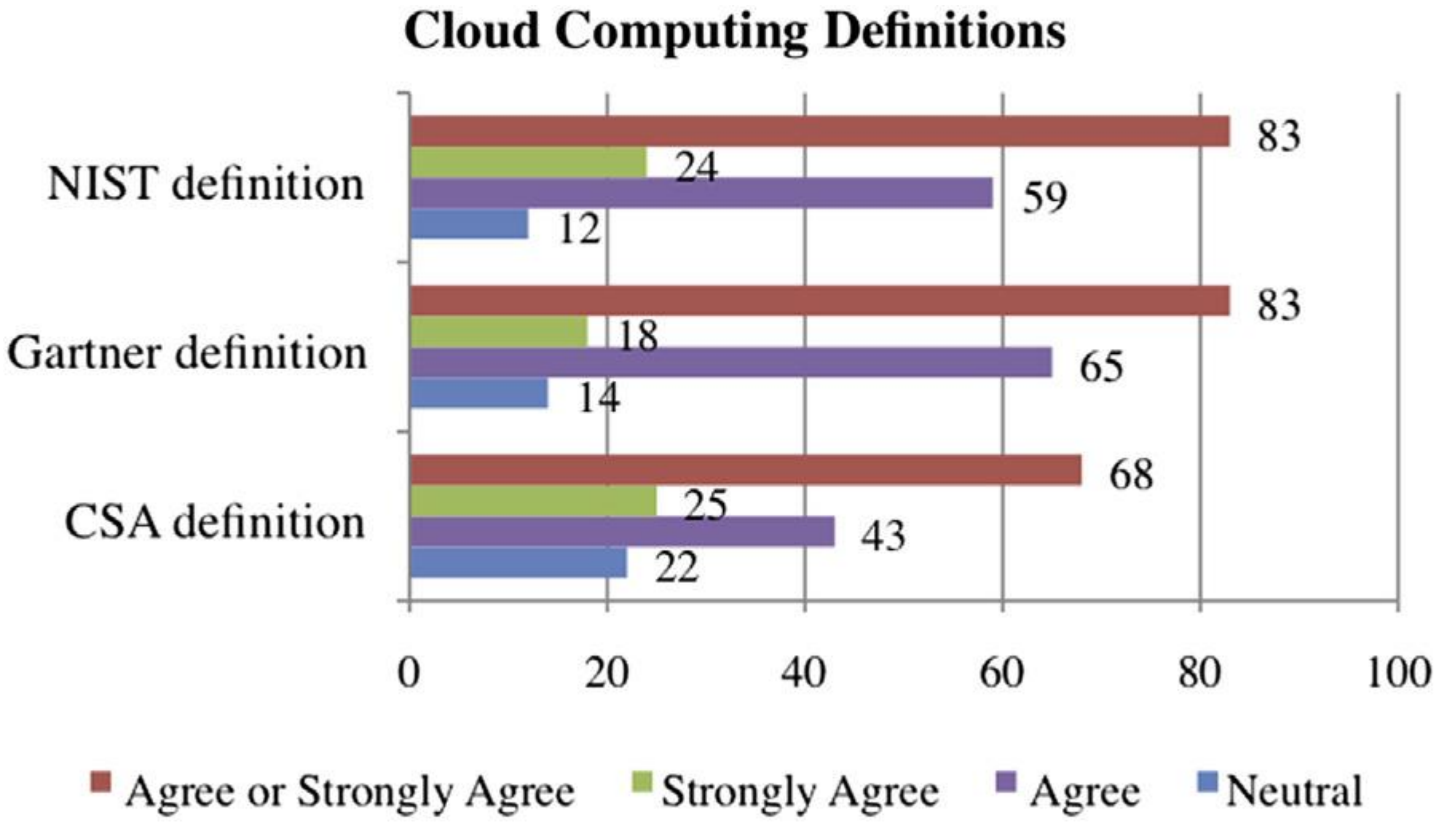
  "Cloud computing is a style of computer where scalable and elastic IT-related capabilities are provided 'as a service' to multiple external customers using Internet technologies."(Gartner, 2009)

- Cloud Security Alliance (CSA) Definition

  "Cloud computing is an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates application and information resources from underlying infrastructure, and the mechanisms used to deliver them. Cloud enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing."(CSA, 2009)

Definition of cloud computing

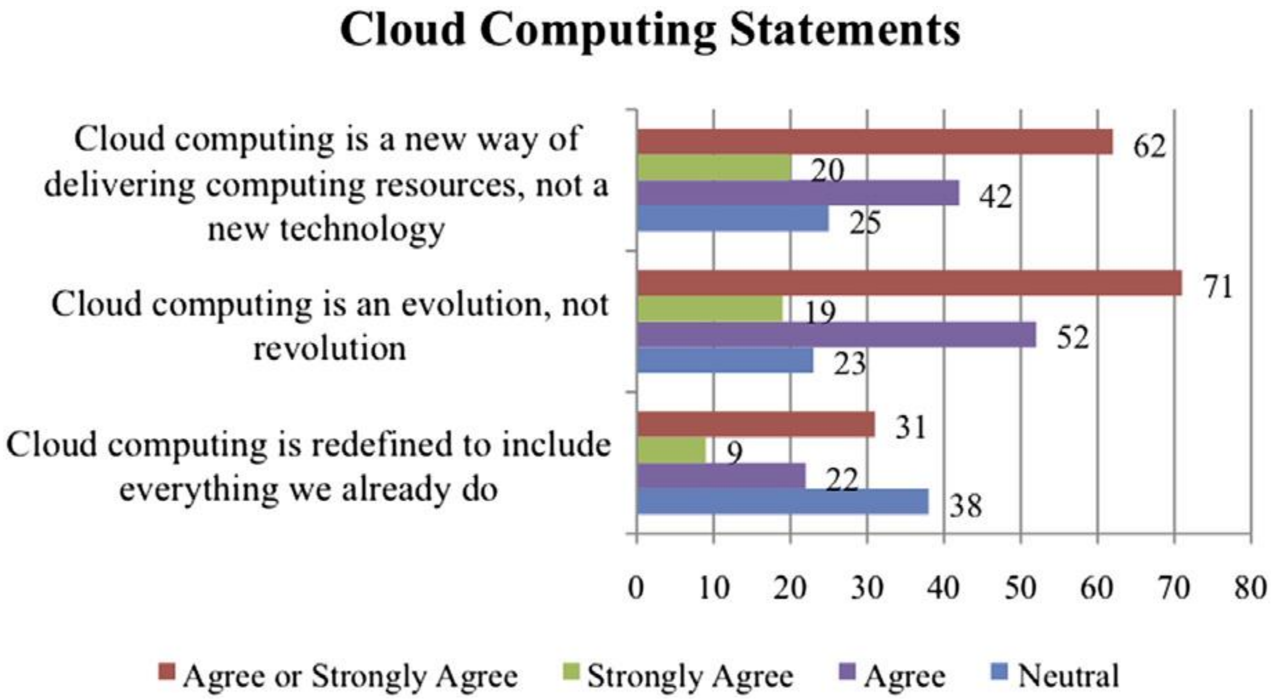
- 126 participants answered



The results show that the respondents have agreed on cloud computing definitions provided by leading international organizations.

Definition of cloud computing

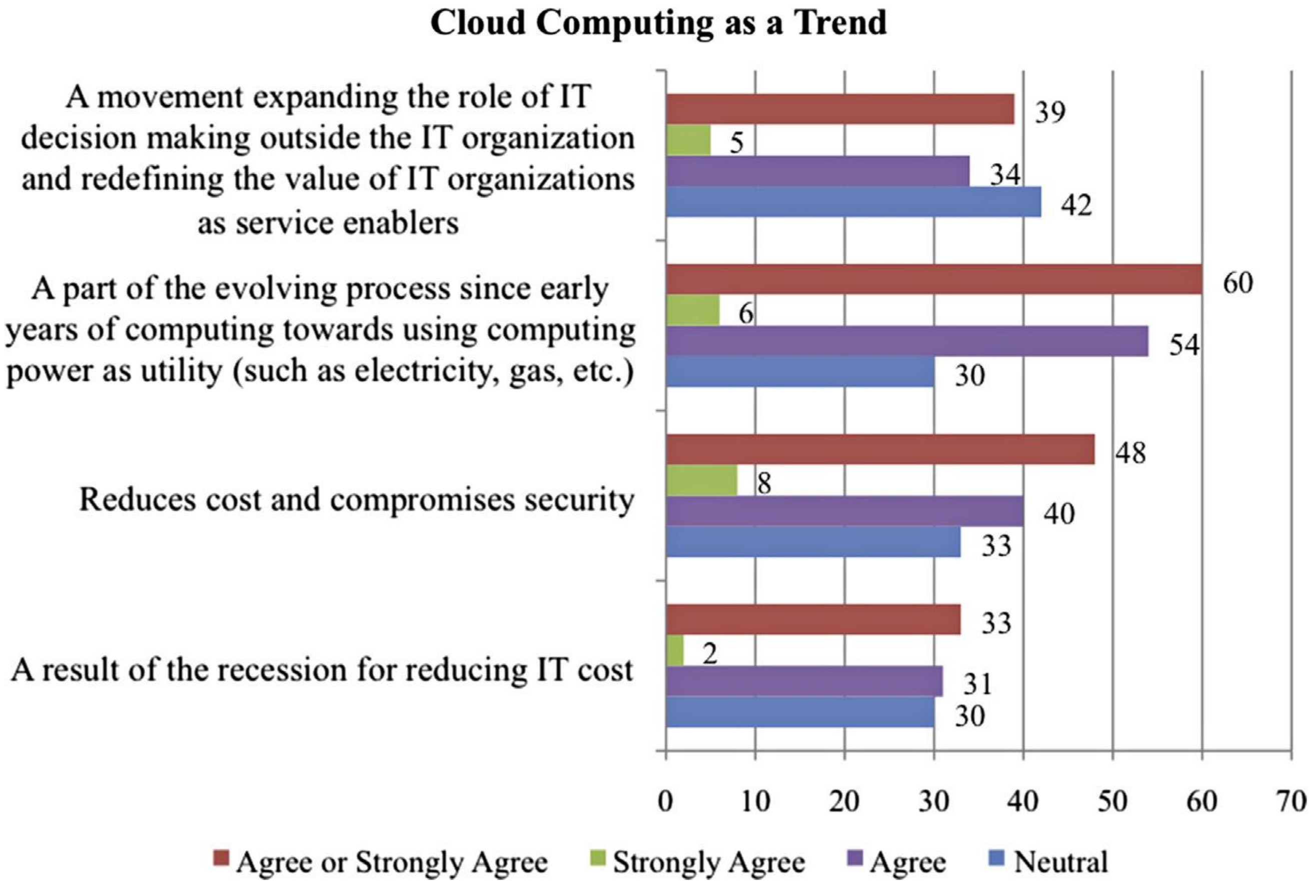
- 126 participants answered



The results show that respondents believe cloud computing is not a new technology, but also not a mere mix of existing technologies. The way it delivers computing resources is new, and this can be the result of the natural evolution of computing.

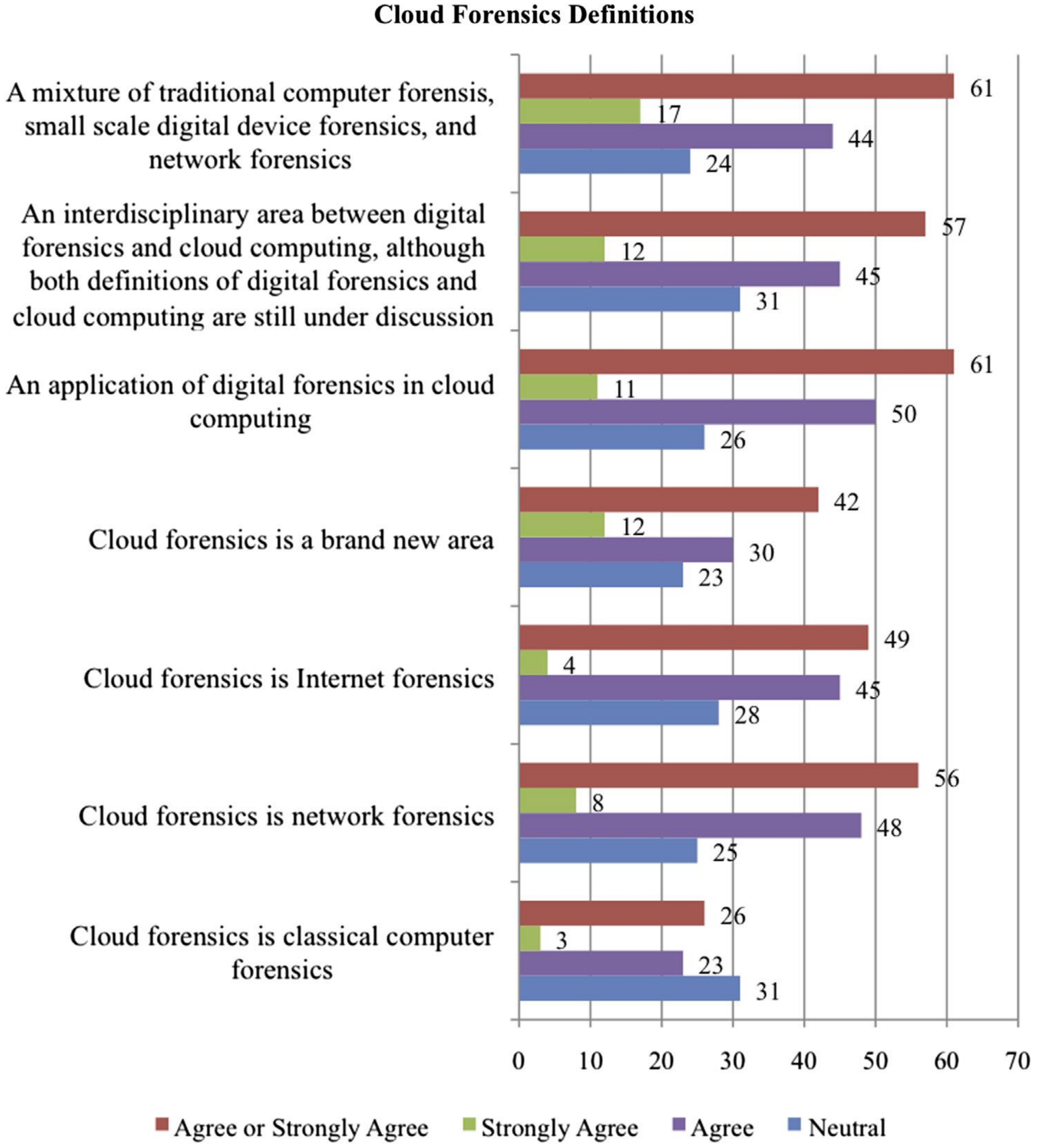
Cloud computing as a trend

- 122 participants answered



Participants do not agree that cost reduction is the primary drive for cloud adoption.

Definition of cloud forensics

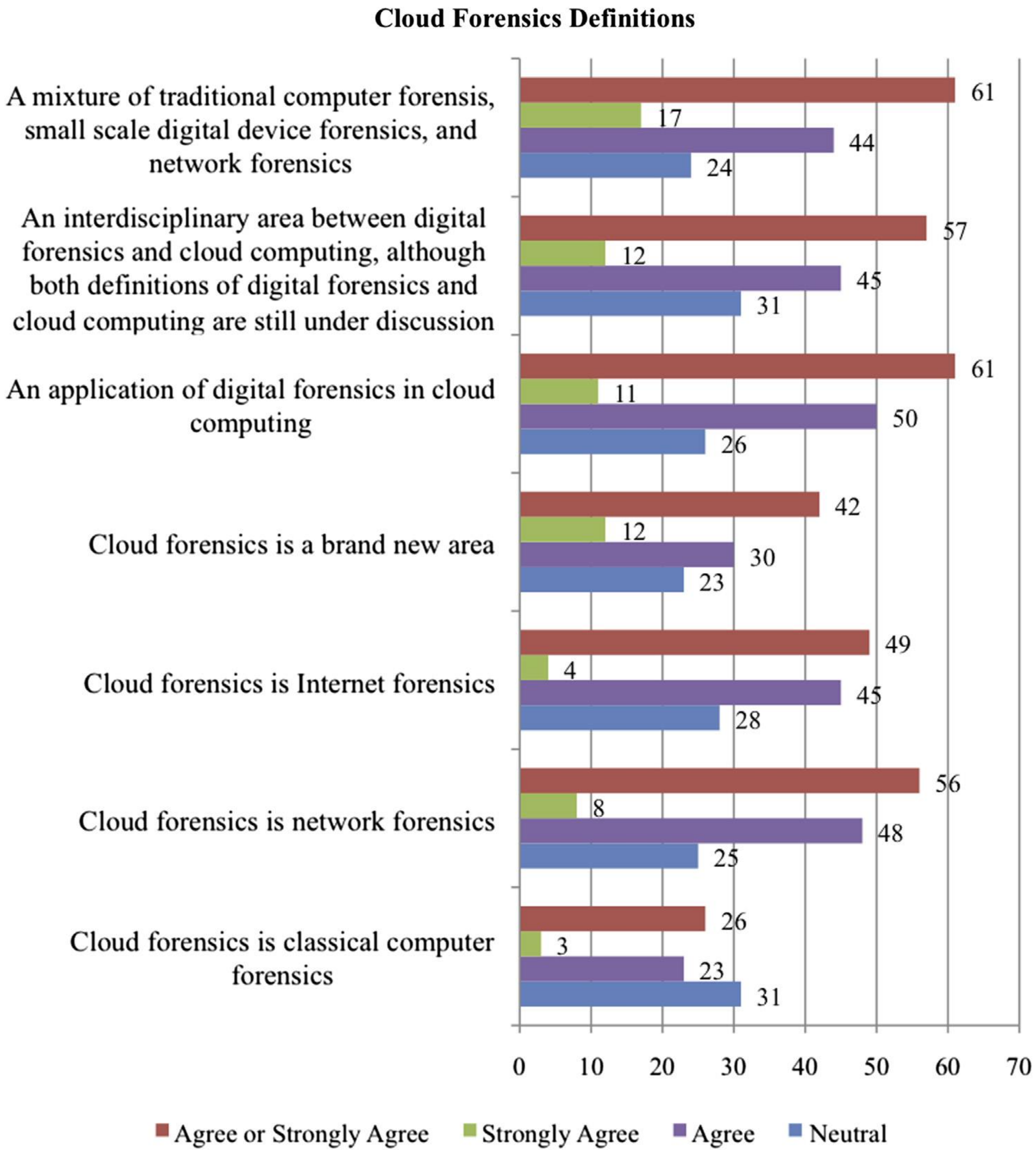


- 123 participants answered

  The respondents believe that cloud forensics is no Internet forensics or classical computer forensics, nor a brand new area.

  It is rather a "mixture" of traditional forensic techniques and their applications in cloud computing environment.

Definition of cloud forensics



- 123 participants answered

  The respondents believe that cloud forensics is no Internet forensics or classical computer forensics, nor a brand new area.

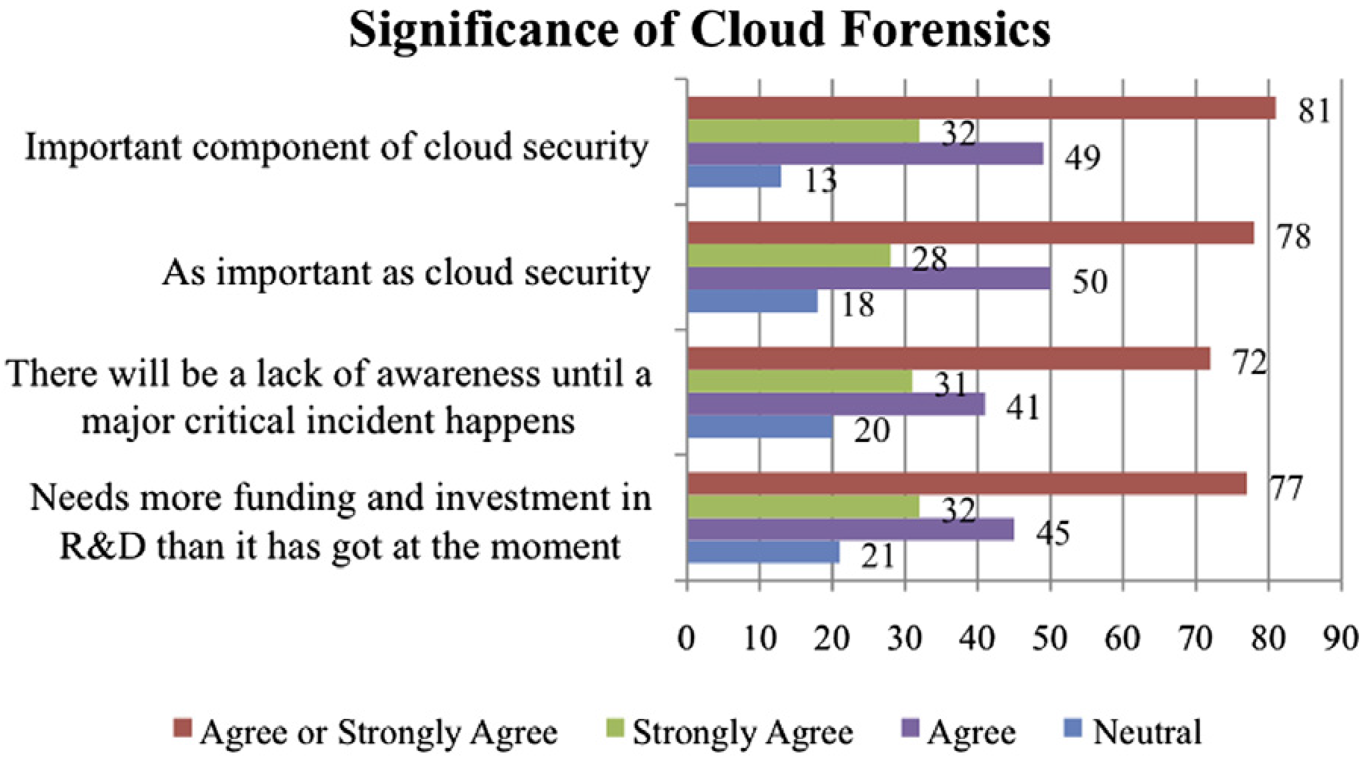
  It is rather a “mixture” of traditional forensic techniques and their applications in cloud computing environment.

- Definition of cloud forensics:

  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.

Significance of cloud forensics

- 122 participants answered



The result show that the respondents have reached consensus on all of the surveyed aspects.

Impact of cloud computing on digital forensic

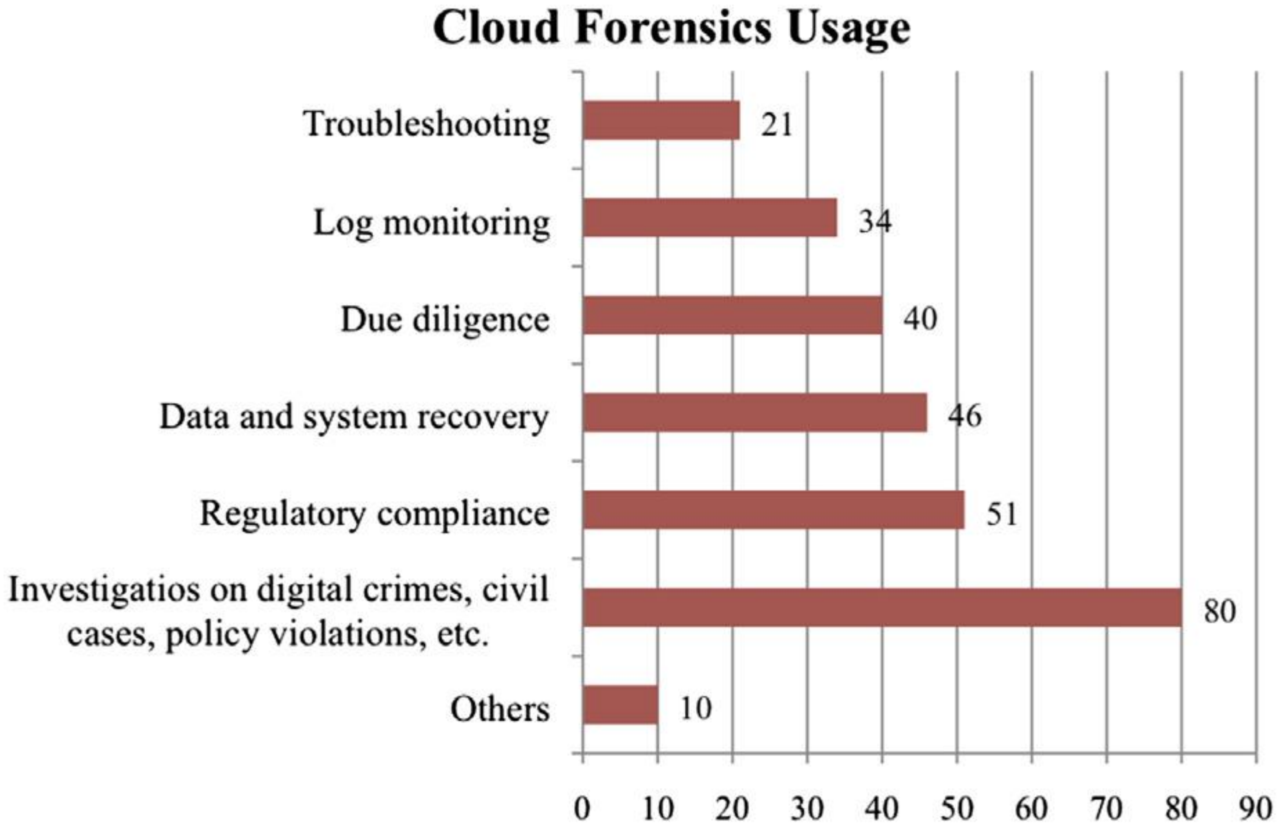
- 101 participants answered
  - 46% of the respondents answered as follows:
    "Cloud computing makes forensic harder"
    - Reduced access to remote and distributed physical infrastructure and storage.
    - Lack of physical control and physical location of data.
    - Lack of standard interfaces.
    - Legal issues including multiple ownership, multiple jurisdictions, and multiple tenancies.
    - Lack of collaboration from the cloud provider(s).
    - Evidence segregation.
    - Data recovery.
  - 37% of the respondents answered as follows:
    "Cloud computing makes forensic easier"
    - Cloud investigations can leverage characteristics of cloud computing, e.g., computing power on demand, elasticity, distributed forensic processing, as well as scalable auditing, reporting, logging, imaging and testing. Forensic implementations in the Cloud can also be cheaper.
    - Cloud investigations will be highly dependent on provider providing digital evidence through centralized administration and management, so there will be less work for the investigator/law enforcement side.
    - Evidences in cloud environments are harder to destroy by the criminals as they may be mirrored to multiple locations.
    - Investigative functionalities can be integrated in cloud implementations, e.g., hashing and imaging are easier in the Cloud.

Cloud forensics dimensions

- 139 participants answered
  - 80% of the respondents agree that there is a "technical" as well as "legal" dimension for cloud forensics.
  - 69% of the respondents agree that there is a "organizational/administrative dimension" for cloud forensics.
  - 43% of the respondents agree that there is a "social dimension" for cloud forensics.
  - 14% of the respondents clicked "other" dimensions.("Political" and "Personal")

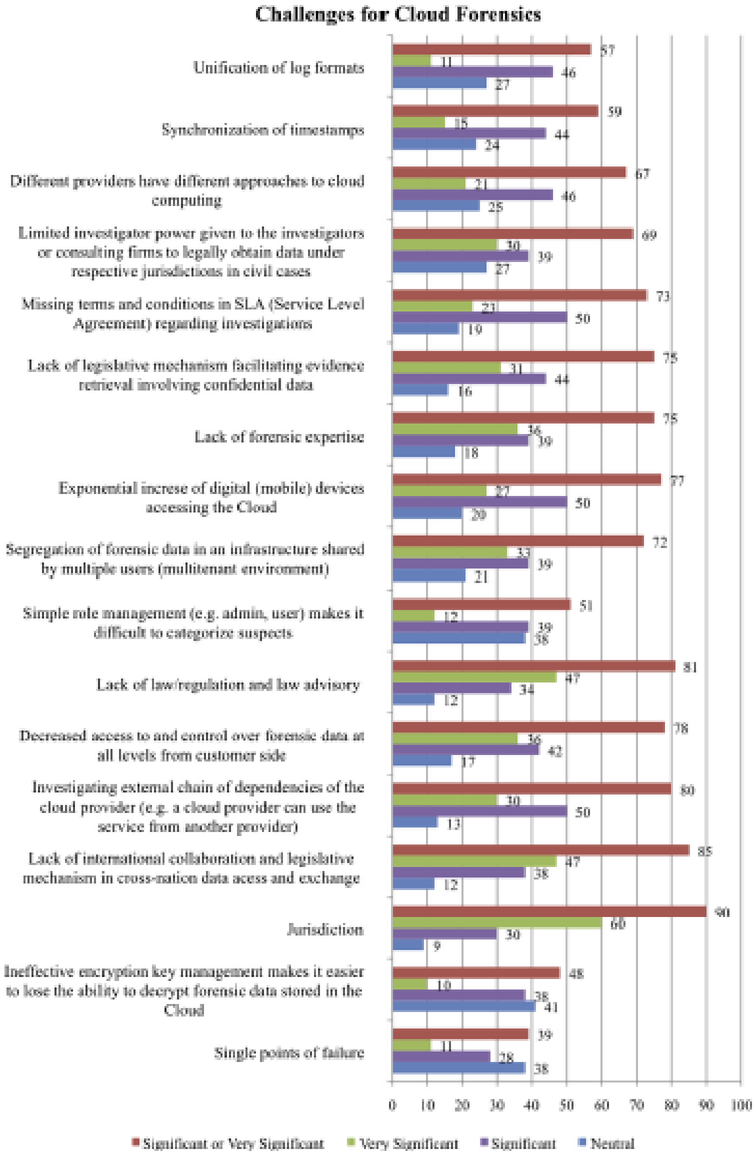
Cloud forensics usage

- 139 participants answered



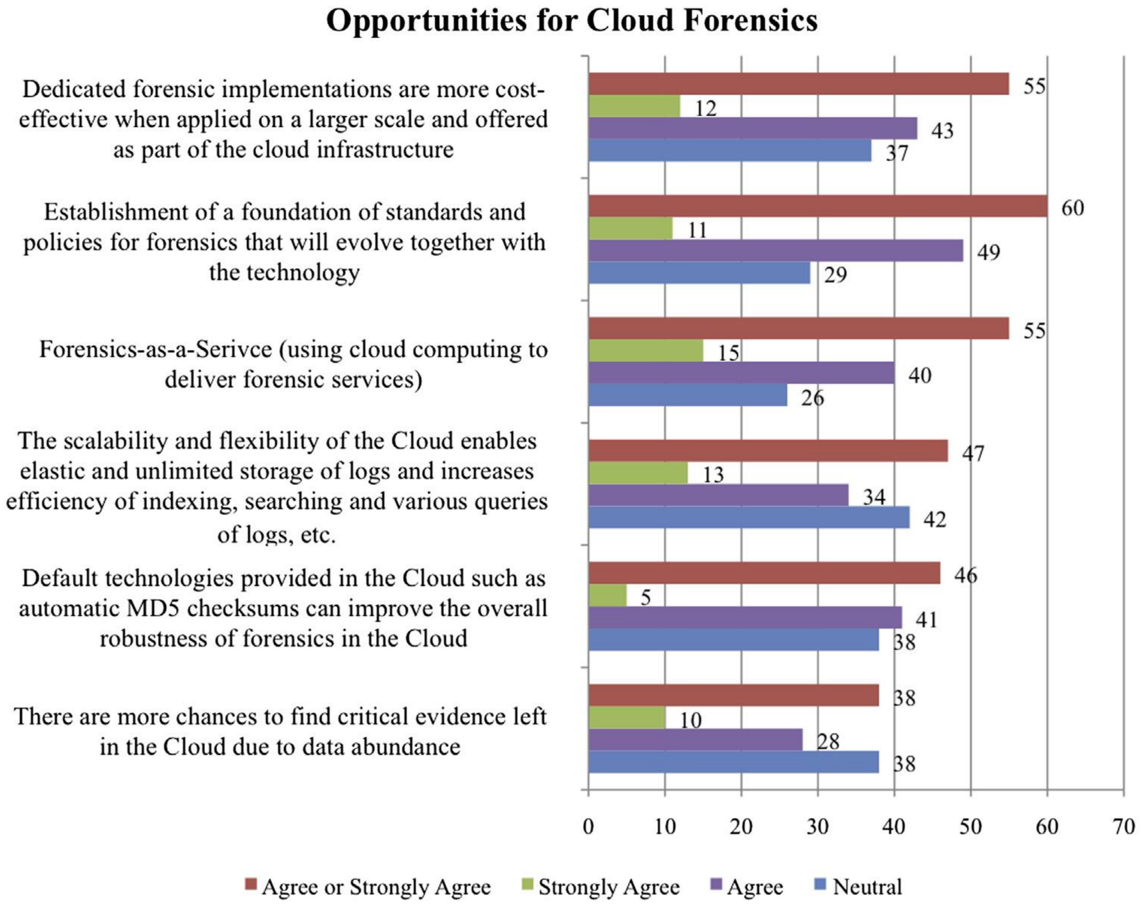
The result show that the respondents have reached consensus on using cloud forensic for “investigations on digital crimes, civil cases, policy violations”.

Challenges



- 106 participants answered
- More than 75% of the repondents
  - Jurisdiction.
  - Lack of international collaboration and legislative mechanism in cross-nation data access and exchange.
  - Lack of law/regulation and law advisory.
  - Simple role management (e.g., admin, user) makes it difficult to categorize suspects.
  - Investigating external chain of dependencies of the cloud provider (e.g., a cloud provider can use the service from another provider).
  - Decreased access to and control over forensic data at all levels from customer side.
  - Exponential increase of digital (mobile) devices accessing the cloud.

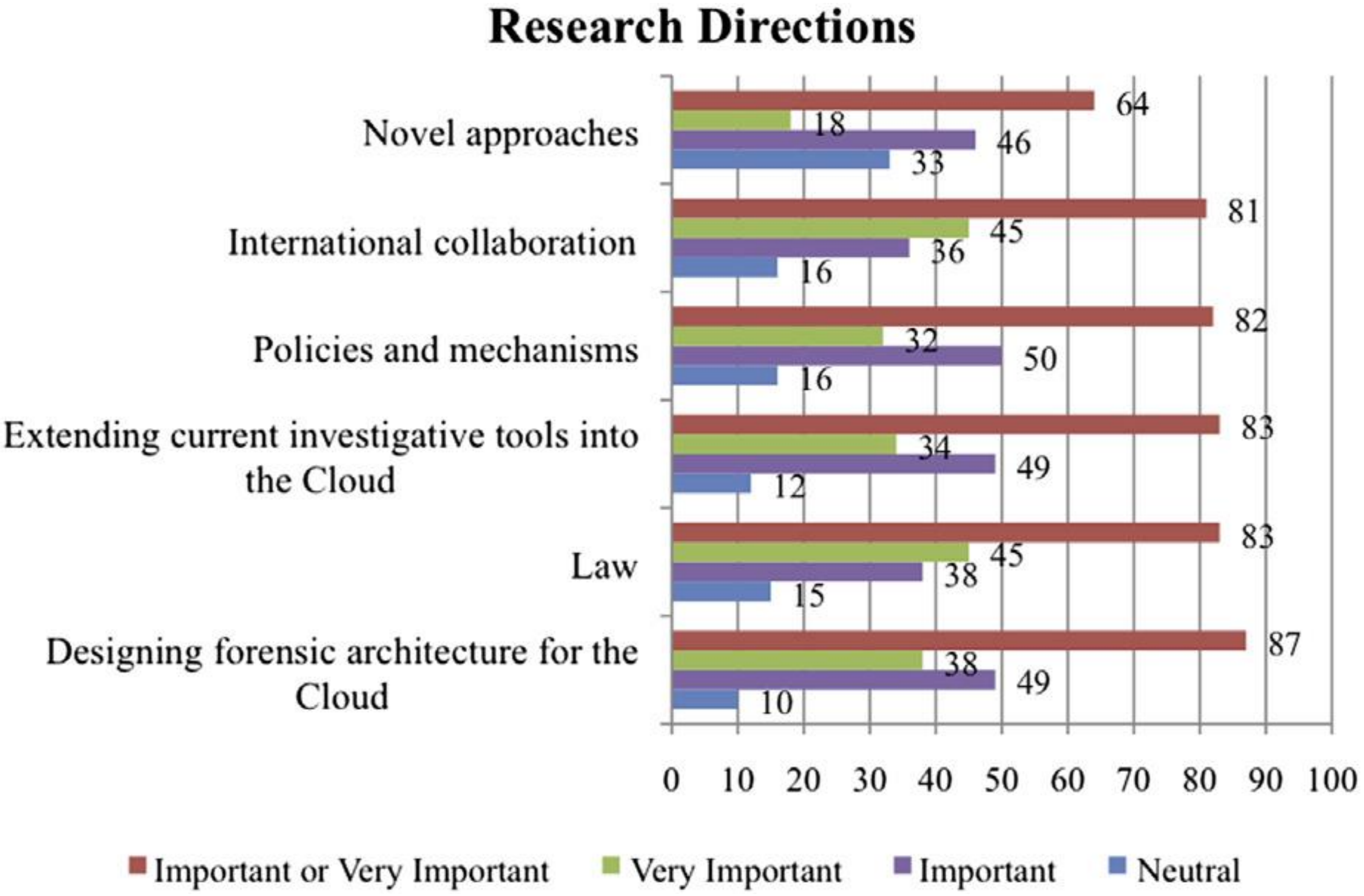
Opportunities



- 105 participants answered
  - Establishment of a foundation of standards and policies for forensics that will evolve together with the technology.
  - Dedicated forensic implementations are more cost-effective when applied on a larger scale and offered as part of the cloud infrastructure.
  - Forensics-as-a-service (using cloud computing to deliver forensic services).

Research directions

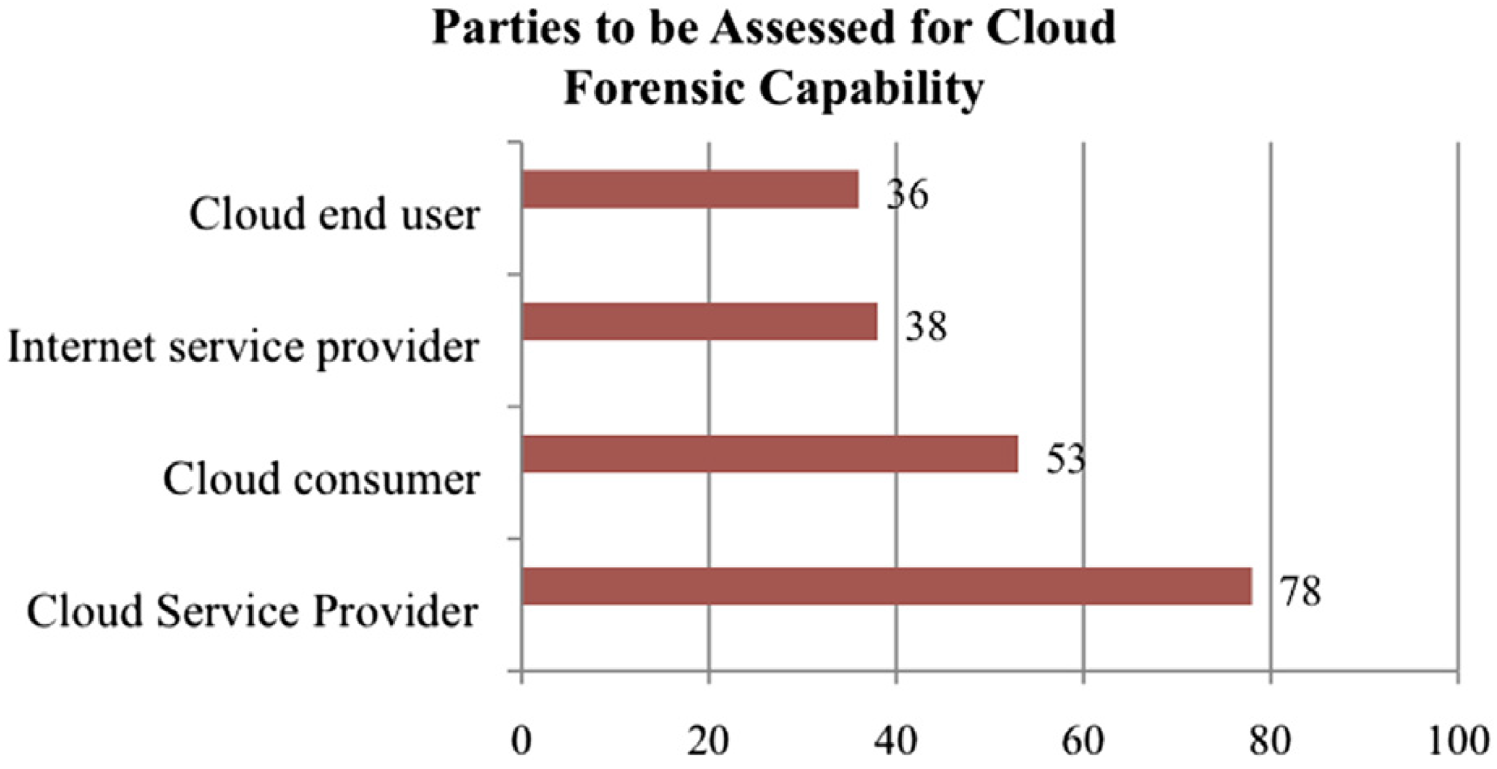
- 106 participants answered



The result strongly show that the area of cloud forensics require significant research efforts.

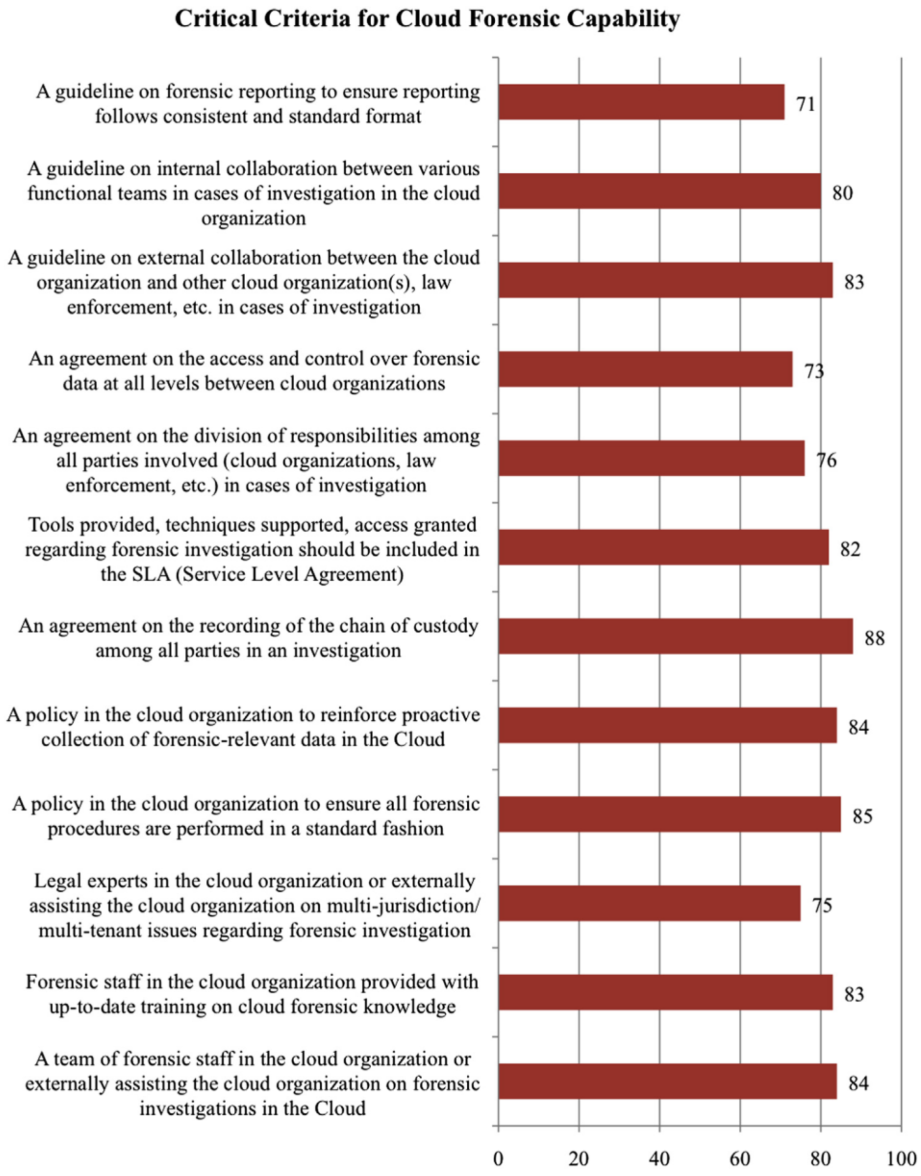
Parties to be assessed for cloud forensic capability

- 111 participants answered



The result strongly show that the Cloud Service Provider and cloud consumer should be assesed.

Guideline, agreement, policy, and staffing importance



- The list of critical criteria for cloud forensic capability can be much further expanded, and the survey results from these questions have strongly indicated the need to further expand this list.

Thank you!