Research on Digital Forensics Based on Private Cloud Computing

Gang Zeng
Dept. of Police Information Technology,
Liaoning Police Academy,
Dalian Liaoning, China
dlzenggang@126.com

outline

* Digital forensics
* Cloud computing
* Conversion of Traditional Digital Forensics into Cloud Computing Service
* Forensics Cloud Computing

1 INTRODUCTION

* Digital forensics
* Procedures of A digital forensics investigation:
  - Identification
  - evidence collection
  - Analysis
  - reporting

2 Cloud Computing

* Service Models of Cloud Computing
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
  - Software as a service (SaaS)

Deployment Models of Cloud Computing

* Public cloud
* Community cloud
* Private cloud
* Hybrid cloud

characteristics of Cloud Computing

* Security and Reliability
* High Availability (shared resources pool)
* Low System Requirements in Client

3 Conversion of Traditional Digital Forensics into Cloud Computing Service

* Limitations of the Traditional Digital Forensics
* limitation of hardware performance
* more maintenances of traditional digital forensic tools
* limitation of the position of the forensic laboratory

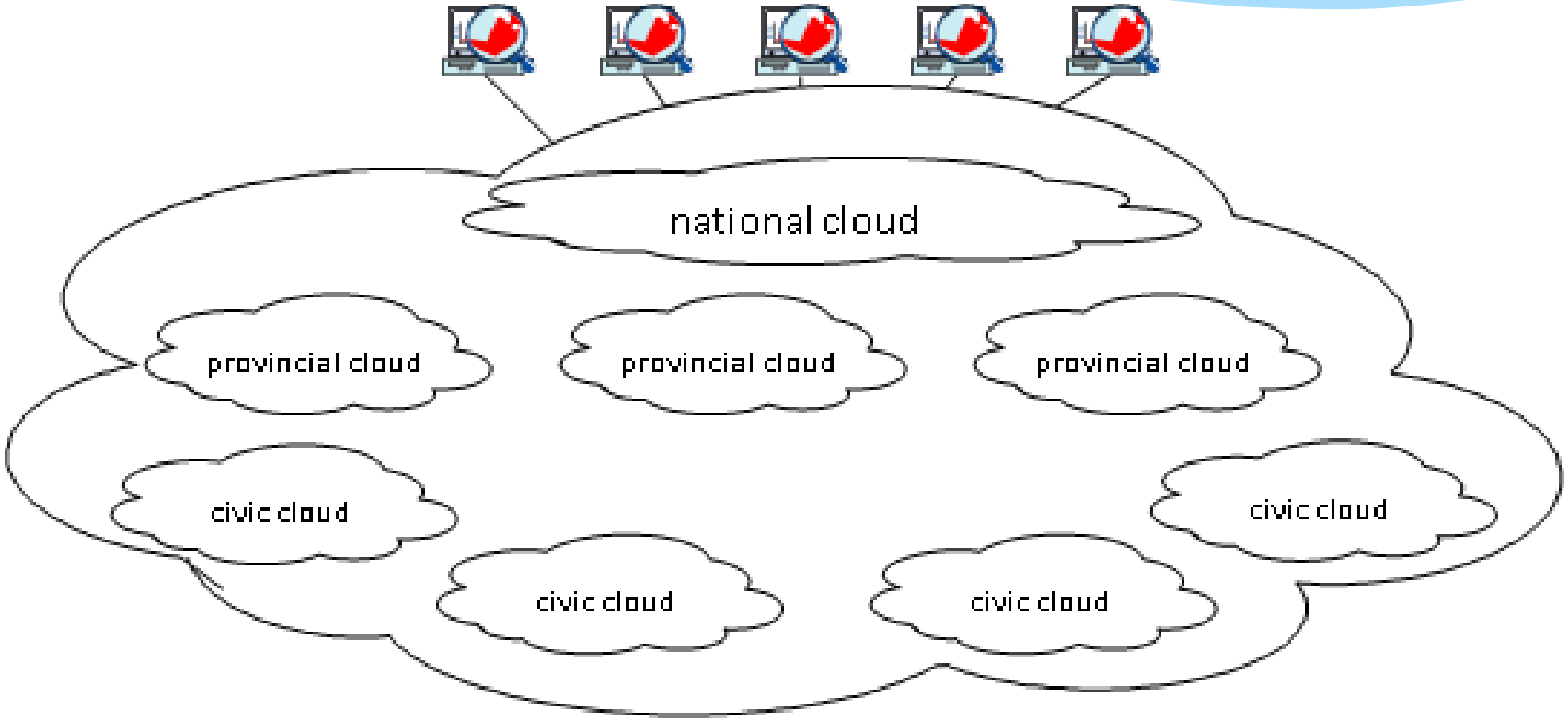
Advantages of Digital Forensics Based on Cloud Computing

* Real-time dynamic forensics
* resources integration
* no limitation to position of the client.
* low requirement for the client
* one or multiple tasks together

Public Cloud or Private Cloud, or others

* Who use the forensic cloud computing?
  * Police or the third party
* Where are the digital evidences stored?
  * Police's intranet
* How is the data being protected?
  * technology and **institution**
* Who access or view the data?
  * Plolice or the third party
* ……

Architecture of Private Forensics Clouds



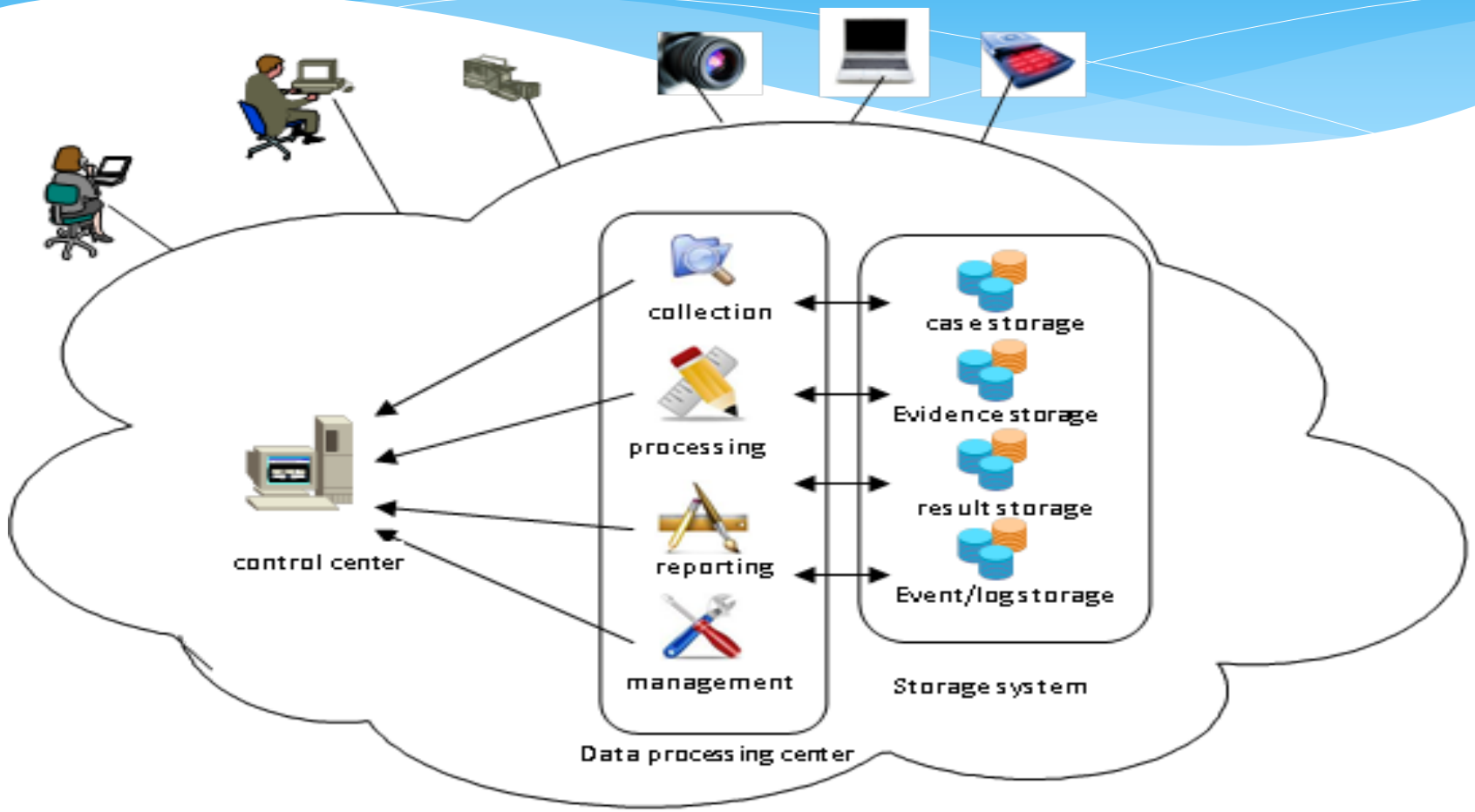
Forensic Cloud Computing

* IaaS Model
* **FaaS Model**

IaaS Model

* IaaS is the simplest model, In this model, the customer uses the virtual machine provided by the CSP to install his own system on it. The system can be used like any other physical computer with a few limitations. Therefore, a lot of investigators use the virtual machine for evidence acquisition, making image of digital evidence from crime scene. The image can be used by forensic tools, such as Encase, FTK, etc.
* At the same time, investigators can load and run the image in a virtual machine. It is dynamic.

FaaS Model


collection
processing
reporting
management
Data processing center
control center
case storage
Evidence storage
result storage
Event/log storage
Storage system

FaaS Model

* control center
* data processing center
* storage system

Procedure of digital forensics in FaaS

* Preparation
* Evidence collection
* Data processing/analysis
* Reporting/Presentation

SUMMARY

* we introduced digital forensics and cloud computing first, then listed the advantages of private forensics cloud computing, discussed private cloud for security, proposed the architecture of private forensics clouds. Finally we proposed forensics procedures of Forensics as a Service(FaaS).

* As a further research, many issues have to be studied, for example, patterns of use, degrees of reliability, privacy and other security, etc.

Thanks