



République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.MIRA-BEJAIA
Faculté des Sciences Exactes
Département d'Informatique
Laboratoire d'Informatique Médicale (LIMED)

THÈSE

Présentée par

AKILAL ABDELLAH

Pour l'obtention du grade de

DOCTEUR EN SCIENCES

Filière : Informatique

Option : Cloud Computing

Thème

Architectures Cloud Forensic Readiness: From a Formal Model to an Implementation

Soutenue le : 05/11/2022

Devant le Jury composé de :

Nom et Prénom	Grade		
M. Aissani Sofiane	MCA	Univ. de Béjaïa	Président
M. Kechadi Mohand Tahar	Prof	UCD, Dublin, Irlande	Rapporteur
M. Farah Zoubeyr	MCA	Univ. de Béjaïa	Examineur
M. Amad Mourad	Prof	Univ. de Bouira	Examineur
M. Omar Mawloud	Prof	Univ. de Bretagne Sud, France	Examineur

Année Universitaire : 2022-2023.

ACKNOWLEDGEMENT

I am grateful to God Almighty, my creator, who gave me the courage to complete this project.

I would like to thank my supervisor Prof. Mohand Tahar Kechadi from University College Dublin for his support and guidance all these years.

I would also like to thank the members of the jury for their valuable time and efforts in examining this thesis. May Dr. Sofiane Aissani, Dr. Zoubeyr Farah, Prof. Mourad Amad and Prof. Omar Mawloud receive my gratitude.

I also wish to thank my family and friends for their constant support and encouragement.

This dissertation is dedicated to my family and my friends.

THESIS CONTRIBUTIONS

In this thesis, we made the following contributions:

RESEARCH PAPERS

1. Abdellah Akilal and M-Tahar Kechadi: *An improved forensic-by-design framework for cloud computing with systems engineering standard compliance*. Forensic Science International: Digital Investigation
DOI: [10.1016/j.fsidi.2021.301315](https://doi.org/10.1016/j.fsidi.2021.301315)
2. Abdellah Akilal and M-Tahar Kechadi: *A Cloud Law Enforcement Request Management System (CLERMS)*. International Journal of Cloud Computing (IJCC). (Under revision)

BOOK CHAPTER

1. Abdellah Akilal and M-Tahar Kechadi: *A Forensic-Ready Intelligent Transportation System*. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering.
DOI: [10.1007/978-3-031-06371-8_39](https://doi.org/10.1007/978-3-031-06371-8_39)

CONFERENCE

1. Abdellah Akilal and M-Tahar Kechadi: *A Forensic-Ready Intelligent Transportation System*. In EAI PFSM 2021 - EAI International Conference on Privacy and Forensics in Smart Mobility, November 24-26, 2021, Portugal

CONTENTS

List of Figures	viii
List of Tables	ix
1 INTRODUCTION	1
1.1 Problem	1
1.2 Motivation	2
1.3 Challenges and Objectives	3
1.4 Contribution	3
1.5 Thesis Organisation	4
2 CLOUD COMPUTING	5
2.1 Introduction	5
2.2 Origins & Definitions	6
2.3 Architecture	8
2.4 Summary	9
3 DIGITAL FORENSICS	10
3.1 Introduction	10
3.2 Digital Forensics	10
3.2.1 Overview & History	10
3.2.2 Definitions	12
3.2.3 Investigation Models	13
3.3 Digital Forensic Readiness	17
3.3.1 Definitions	17
3.3.2 Processes and Models	18
3.3.3 DFR standards	20
3.4 Summary	23
4 CLOUD FORENSIC	24
4.1 Introduction	24
4.2 Overview	24
4.3 Opportunities	25
4.4 Challenges	26
4.4.1 Systematic Literature Review	26
4.4.2 Challenges Classification	27

4.5	Cloud Forensic Readiness	30
4.5.1	Definition	31
4.5.2	CDFR Architecture	31
4.6	Summary	32
5	FORENSIC-BY-DESIGN	33
5.1	Introduction	33
5.2	Systematic Literature Review	33
5.3	FbD Frameworks	38
5.4	Opportunities and Challenges	40
5.4.1	Opportunities	40
5.4.2	Challenges	44
5.5	Research Gaps	47
5.6	Hypothesis	47
5.7	Summary	48
6	AN IMPROVED FORENSIC-BY-DESIGN FRAMEWORK	49
6.1	Introduction	49
6.2	Hypothesis arguments	49
6.2.1	Key factors & Challenges Mapping	50
6.2.2	Persistent Challenges Filtering	55
6.2.3	FbD alignment with SE standards	57
6.3	The proposed framework	60
6.3.1	Motivations	60
6.3.2	General guidelines	61
6.3.3	Key factors and best practices	62
6.3.4	System life cycle	64
6.4	Proposed framework validation	67
6.4.1	Hypothetical case study	67
6.4.2	Real-world project	71
6.5	Opportunities and limitations	73
6.6	Summary	74
7	A FORENSIC-READY INTELLIGENT TRANSPORTATION SYSTEM	75
7.1	Introduction	75
7.2	Economic Impact	75
7.3	Security and Incidents	76
7.3.1	Attackers	76
7.3.2	Attack vectors and surface	77

7.3.3	Real world attacks	79
7.4	ITS DFR	82
7.5	Architecture & Standards	82
7.5.1	Selected Architecture	83
7.6	FR-ITS Opportunities	85
7.6.1	Methodology	85
7.6.2	Forensic-by-design	86
7.6.3	Concerns	86
7.6.4	Readiness	86
7.7	FR-ITS Challenges	87
7.7.1	Boundaries	87
7.7.2	Digital vs Physical	87
7.7.3	Requirements elicitation	88
7.7.4	Scale and volumes	88
7.7.5	Standards and practices	88
7.8	Summary	89
8	LE EVIDENCE ACCESS IN THE CLOUD	90
8.1	Introduction	90
8.2	Multi-jurisdictions	91
8.3	Formal channels for cross-borders data access	91
8.4	Transparency reports and LE guidelines	92
8.5	LE requests management system	93
8.6	Legal request processing Issues	94
8.7	Problem statement	95
8.8	Goals and Scope	96
8.9	Summary	96
9	CLOUD LAW ENFORCEMENT REQUEST MANAGEMENT SYSTEM	97
9.1	Introduction	97
9.2	The Proposed solution	97
9.2.1	LE request processing flow	98
9.2.2	Architecture definition	99
9.2.3	System requirements	102
9.3	Prototype design & development	102
9.4	Cloud deployment	104
9.5	Prototype validation	106
9.6	Economic assessment	107

9.7 Opportunities & limits	108
9.8 Summary	109
10 CONCLUSION AND FUTURE WORK	110
10.1 Conclusion	110
10.2 Future Work	112
 BIBLIOGRAPHY	 113

LIST OF FIGURES

Figure 2.1	Cloud Computing service models (M. L. Badger et al., 2012). . .	7
Figure 2.2	NIST Cloud Computing reference architecture (Liu et al., 2011).	9
Figure 3.1	NIST Digital Forensic Investigation model (Kent et al., 2006). .	14
Figure 3.2	NIST Digital Forensic Investigation model (Palmer et al., 2001).	15
Figure 3.3	Ciardhuái Digital Forensic Investigation model (Ciardhuáinand, 2004).	16
Figure 3.4	Incident investigation principles and processes groups (<i>Information technology — Security techniques — Incident investigation principles and processes</i> 2015).	21
Figure 3.5	Readiness processes group (<i>Information technology — Security techniques — Incident investigation principles and processes</i> 2015).	22
Figure 4.1	CFRS reference architecture (De Marco, M.-T. Kechadi, and Ferrucci, 2014).	31
Figure 5.1	A conceptual Forensic-by-design framework (Rahman, Glisson, et al., 2016).	38
Figure 5.2	A Medical Cyber-Physical System Forensic-by-design framework (Grispos, Glisson, and Choo, 2017).	39
Figure 5.3	An integrated cloud incident handling and forensic-by-design model (Choo, Herman, et al., 2016).	42
Figure 6.1	Potential DFI scenario 1. Adapted from (Ruan and Carthy, 2013a)	51
Figure 6.2	Potential DFI scenario 2. Adapted from (Ruan and Carthy, 2013a)	51
Figure 6.3	Potential DFI scenario 3. Adapted from (Ruan and Carthy, 2013a)	51
Figure 6.4	A system of interest structure.	58
Figure 6.5	A Forensic-by-design framework for Cloud computing systems.	61
Figure 6.6	ARC-IT architecture (DoT, 2021e).	71
Figure 7.1	ITS security attack vectors (Huq, Vosseler, and Swimmer, 2017).	78
Figure 7.2	Sign hack (Kelarestaghi et al., 2018).	80
Figure 7.3	M.T.A time keeping systems ransomware attack (Nypost, 2021).	81
Figure 7.4	Remote Car Hijacking (Miller, 2019).	81
Figure 7.5	The ARC-IT Physical view (DoT, 2021e).	84

Figure 8.1	Example of an US MLAT process for Electronic Evidence (Lin and Fidler, 2017).	92
Figure 9.1	LE request processing workflow.	99
Figure 9.2	An abstract architecture for a law enforcement requests management system.	100
Figure 9.3	A Cloud Law Enforcement Request Management System.	103
Figure 9.4	CLERMS deployment on an IaaS infrastructure.	104
Figure 9.5	Grr-server administration user interface.	105
Figure 9.6	Monitoring, logs ingestion, and threat hunting via Kibana dashboards.	105
Figure 9.7	Online LE request pre-submission portal	106
Figure 9.8	Kirjuri open source case management User Interface.	106

LIST OF TABLES

Table 4.1	Cloud Forensic challenges search results.	27
Table 4.2	Cloud Forensic challenges selected papers comparison.	28
Table 4.3	Cloud Forensics challenges classification (Herman et al., 2020).	30
Table 5.1	Forensic-by-design search results	35
Table 5.2	FbD selected papers comparison (part1).	36
Table 5.3	FbD selected papers comparison (part2).	37
Table 5.4	FbD issues and challenges.	46
Table 6.1	Mapping (Herman et al., 2020) CF challenges with (Rahman, Glisson, et al., 2016) framework key factors.	54
Table 6.2	FbD Key factors associated standards and best practices.	64
Table 6.3	The proposed framework's key factors integration.	65
Table 6.4	Designing an ITS (Vanets recommendations).	69
Table 6.5	Designing an ITS (Cloud Broker recommendations).	70
Table 6.6	Mapping between the ARC-IT properties and the proposed framework.	72
Table 8.1	CSP's Transparency reports and LE guidelines attributes.	93
Table 9.1	Economic assessment of CLERMS deployment solution for a customer plane of 7000 nodes.	108

ACRONYMES

CC	Cloud Computing
CCS	Cloud Computing Systems
CSA	Child Sexual Abuse
CSP	Cloud Service Provider
CSC	Cloud Service Consumer
CB	Cloud Broker
CA	Cloud Auditor
CR	Cloud Carrier
CF	Cloud Forensics
CDFR	Cloud Digital Forensic Readiness
CPCS	Cyber-Physical Cloud Systems
CFRA	Cloud Forensics Reference Architecture
CFbDF	Cloud Forensic-by-Design Framework
CLERMS	Cloud Law Enforcement Request Management System
C-ITS	Cooperative Intelligent Transportation System
DF	Digital Forensics
DFI	Digital Forensic Investigation
DFR	Digital Forensic Readiness
DMTF	Distributed Management Task Force
FbD	Forensic-by-Design
FR-ITS	Forensic-Ready Intelligent Transportation System

IS	Information System
ITS	Intelligent Transportation System
IaaS	Infrastructure as a Service
IT	Information Technology
LE	Law Enforcement
MCPS	Medical Cyber-Physical Systems
OVF	Open Virtualization Format
OIA	Office of International Affairs
P2P	peer-to-peer
PaaS	Platform as a Service
SbD	Security-by-Design
SSE	System & Software Engineering
SLA	Service Level Agreement
SaaS	Software as a Service

INTRODUCTION

1.1	Problem	1
1.2	Motivation	2
1.3	Challenges and Objectives	3
1.4	Contribution	3
1.5	Thesis Organisation	4

1.1 PROBLEM

Technological advancements are affecting peoples' daily life for the best as for the worst. We are in an era of *information* and communication, where everyone and everything is connected through invisible links. The pervasiveness of emerging technologies rely on the ability to ensure a transparent yet effective communication and computation. *Anywhere* and *anytime* are the key factors of the omni-connectivity that we are living in, which may not be affordable or feasible without the emergence of new paradigms such as Cloud computing.

Cloud computing (Mell and Grance, 2011) is a computation model that enables an ubiquitous, on-demand access —at a pay per usage rate— to *shared* resources, with minimal management effort. Relaying on *virtualisation*, this model offers the illusion of limitless resources to often multi-tenants customers. Scalability, flexibility, interoperability and other key characteristics of this model are easing the design and development of Cloud services that are reachable to end-users anywhere, anytime, and through multiple devices.

Cloud services and other related technologies are transparently present in every aspect of our daily life. From a Smart-watch to a Smart city, every Smart labelled technology requires connectivity and computation that are ensured by a Cloud computing infrastructure. Although it makes our daily lives easier, the worst may happen.

Security incidents are not a matter of *if*, but *when* (Rahman, Glisson, et al., 2016). Due to the pervasiveness of these new technologies, the likelihood of a security incident (or cyber-crime) occurring in the digital world and having impact on physical assets is not negligible. Without being alarmist, such incidents are already occurring in the real world (Miller, 2019).

When the worst happens, an investigation is required to either catch the culprit or to prevent future occurrences. However, the conducted investigation must rely on scientifically proven methods.

Digital Forensics (Palmer et al., 2001) is a *science* that empowers investigators with required proven methods for the preservation, collection, validation, and analysis of digital evidence.

Even if this science relays on proven methods it still requires evidence. Indeed, no investigation is feasible without evidence.

Enabling an organisation (or a system) with the *ability* to collect admissible digital evidence, while minimising the cost of an investigation is the sole purpose of the Digital Forensic Readiness domain. When an organisation (or a system) possesses such ability it is said to be *forensic-ready*. More precisely, *forensic-ready* is the conceptualisation of a time state in which the ability to collect digital evidence is present.

Enabling Cloud computing systems with the due Digital Forensic Readiness capabilities may be feasible. As such, this dissertation discusses the design and conception of *forensic-ready* Cloud computing systems.

1.2 MOTIVATION

It is undoubtedly clear that Cloud computing is empowering and igniting the emergence of more and more pervasive technologies. However, the potential of a digital incident having impact on physical assets calls urgently for tailored digital forensic techniques, methods and tools especially designed and elaborated for these environments.

This concern has led the researchers to establish a new area in digital forensics which is Cloud Forensics (CF) (Ruan, Carthy, T. Kechadi, and Crosbie, 2011). Certainly, CF presents many opportunities for the DF as well as for CC, such as the perspective of scaling traditional DF tools, or even more impulsing the venue of Forensic as a Service. However, CF challenges are very complex, non linearly dependant, and often span across multiple dimensions (technical, organisational, and legal). For example, the multi-jurisdiction challenge, which is a legal one, does have an impact on digital evidence localisation, as data is stored and processed in multiple data centres around the world. For this issue alone, the *elementary* task of collecting evidence may be hard to achieve.

More importantly, as stated before, no investigation is feasible without evidence. Thus, the need for digital forensic readiness capabilities for Cloud computing systems.

Even if there are numerous works (De Marco, M.-T. Kechadi, and Ferrucci, 2014; Kebande and H. S. Venter, 2017; Kebande and H.S. Venter, 2015; Ruan and Carthy, 2013b; Trenwith and H.S. Venter, 2013) on the aforementioned topic, there are still some insufficiencies, which are essentially due to CF challenges.

Tackling all CF challenges and issues at once in order to achieve the forensic readiness of Cloud computing systems may seem as an option. However, such option may be a difficult task by itself, as there are more than 65 CF challenges and nine categories. Focusing on a single challenge or a category of challenges may also be considered. However, there may be another alternative (FbD) (Rahman, Glisson, et al., 2016).

The third alternative (Forensic-by-Design) constitutes a shift in DFR perspective. While previous works focused on “*in production*” systems, this new paradigm aims towards the design and the development of *forensic-ready* systems (*i.e., systems that will possess the ability to collect*

admissible digital evidence from their design to their retirement), However this paradigm is at its infancy.

Therefore, this dissertation discusses the three pathways: (1) investigating the feasibility of enabling Cloud computing systems with the due DFR capability through the mitigation of all the CF challenges, (2) Focus on a single, or a category, of CF challenges, (3) think outside the box.

1.3 CHALLENGES AND OBJECTIVES

There are several challenges to face. In fact, CF already contains nine categories and 65 issues (Herman et al., 2020). Moreover, CC technologies are advancing rapidly, leading to multiple data formats, devices, protocols, etc. Furthermore, orbiting technologies (*i.e.*, *systems or computation models that rely on CC*), such as Fog computing, IoT, and other labelled Smart-X innovations are amplifying the already identified issues.

Throughout this myriad of challenges, we may confidently say that the work presented in this thesis has achieved some important objectives, such as: (1) investigate the efficiency of Forensic-by-Design in Cloud computing systems, (2) proposition of an improved framework for *forensic-ready* Cloud computing systems, (3) assessment of the opportunities that may emerge from applying the FbD strategy to Intelligent Transportation Systems, (4) Introducing a technical capability to ease one of the CF legal challenges (multi-jurisdictions).

1.4 CONTRIBUTION

The first contribution of this doctoral thesis is the enunciation of an hypothesis on the efficiency of Forensic-by-Design for some types of open boundaries systems, and then proving it. Afterwards, we provide an improved framework for Forensic-by-Design Cloud computing with systems engineering standard compliance.

The validation of the proposed framework was done through an hypothetical case study and the analysis of a real world project (DoT, 2021e), which is a reference architecture for Intelligent Transportation System.

The second contribution goes along the first, as we clearly enunciate the concept of *forensic-ready* as being a system's temporal state, then we assess the potential of using FbD strategy to design and develop a *forensic-ready* Intelligent Transportation System.

The third contribution focuses on easing one of the CF legal challenges (Multi-jurisdictions). More precisely, our proposition aims to enhance the ability of a CSP to manage and respond to law enforcement requests.

1.5 THESIS ORGANISATION

This thesis is structured as follows: Chapter 2 presents an overview of Cloud computing. Digital forensic and Digital Forensic readiness are described in Chapter 3. Chapter 4 provides an overview of Cloud Forensics and Cloud Forensics Readiness; In Chapter 5 a presentation of Forensic-by-Design paradigm is given along with its definition, architectures, challenges, opportunities, and research gaps. Later on, in Chapter 6, An Improved Framework for Forensic-by-design Cloud computing systems is introduced. Chapter 7 describes an assessment of Forensic-ready Intelligent Transportation System. An overview of Law Enforcement access to digital evidence in Cloud computing is presented in Chapter 8; Chapter 9 describes a Cloud Law Enforcement Request Management System; Some conclusion and future work are presented in Chapter 10 that closes the dissertation itself.

CLOUD COMPUTING

2.1	Introduction	5
2.2	Origins & Definitions	6
2.3	Architecture	8
2.4	Summary	9

2.1 INTRODUCTION

In this chapter, we will introduce the first paradigm that is related to this thesis, and which is Cloud Computing (CC).

Nowadays, these words “*Cloud Computing*” (CC) are widely used even by the non IT community. This new paradigm is used to refer to the technological evolution that allows a user to connect and consume a service in a remote fashion through multiple devices (PC, smart phone, smart watches, etc.), anytime and anywhere. However, tracing the origins of this new paradigm is a bit more difficult then it seems. In fact, this paradigm results from the conjugate efforts of multiple researchers and the advancements made in several computer science topics, such as distributed computing, networks, virtualisation and web services.

Nonetheless, even if organisations and end-users are not fully aware of: (1) how the consumed services (or resources) are being provisioned and orchestrated, (2) where their data is located and stored, this does not refrain them from taking advantage of the inherent elasticity of CC and therefore adopting it.

Indeed, Cloud Computing economic incentives’ are multiple. Beyond the ability of an enterprise to outsource parts of its Information System (IS), it is also offered a payment per usage model. Therefore empowering them to cut some of their IT expenditure both in infrastructure investments and human resources salaries.

Finally, according to Gartner, 2019, worldwide public cloud service revenue will grow from \$182.4 billions in 2018 to \$331.2 billions in 2022. Despite the forecited advantages, this migration is not without risks. In fact, Cloud Service Provider (CSPs) power outages and incidents may have financial and reputation impacts on their consumers’ business (Lyod, 2017, 2018; Norton, 2019). Indeed, incidents and security breaches are not a matter of “*If*”, but “*When*” (Rahman, Glisson, et al., 2016).

In the following, we discuss the origins of CC and its associated definitions and architectures.

2.2 ORIGINS & DEFINITIONS

Many definitions have been associated with the CC paradigm (see Buyya, Yeo, and Venugopal, 2008; Vaquero et al., 2008). However, the one that seems to gain consensus, and is widely cited is the one by Mell and Grance, 2011. The authors state that: *“Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable Computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models”* (Mell and Grance, 2011).

The above mentioned definition includes all the properties that distinguish CC for other services' delivery technologies, and which are :

1. **On-demand self-service.** One of the main characteristics of CC is the fact that it provides Cloud Service Consumer with the ability to provision by themselves the needed computing capabilities (resources), without requiring a human interaction with a provider.
2. **Broad network access.** Cloud services and resources are made available for consumers through the network. Additionally, these offered capabilities may be used by a heterogeneous and diverse client platforms (e.g., mobile phones, tablets, laptops, and workstations).
3. **Resource pooling.** In this computation paradigm, the provider's resources (processing, storage, network bandwidth) are pooled to serve multiple consumers through a multi-tenant model. Physical (or virtual) resources are allocated or liberated in accordance with the customer's demand. However, a customer has no knowledge or control over the exact location of the provisioned resource, with the exception of some cases (deployment model) where a customer may specify computation zone (country, region, datacenter).
4. **Rapid elasticity.** From a CSC perspective, the available resources and capabilities may seem unlimited, provisioned and released on demand in any quantity at anytime. Indeed, CC is characterized by the ability to scale the consumer's allocated resources up and down elastically and on demand.
5. **Measured service.** Metrics and measures are associated with the provided resources for multiple purposes, such as monitoring, control, reports, billing, and ensuring a transparent relation between the provider and the consumers in regards to the allocated resource.

In addition to the above cited five key characteristics, Mell and Grance, 2011 definition states three service models and four deployment models.

As for the service models (see Figure. 2.1), there are three ones: Software as a Service, Platform as a Service, and Infrastructure as a Service. Further details on these models may be found in M. L. Badger et al., 2012.

For the first instance, with the Software as a Service ([SaaS](#)) model, consumers are offered access to applications running on the provider infrastructure. Access to those applications is granted via browsers and application programming interface. However consumers do not control nor do they manage the underlying cloud infrastructure (storage, networks, etc.) of the consumed service. In most cases only configuration and setting are offered to the consumer to personalize its usage of the cited applications.

In the [PaaS](#) model, consumers may create or deploy their (or acquired) applications using programming languages and libraries that are supported by the provider. However, as for the [SaaS](#) model, the consumer does not control nor does it manage the underlying cloud infrastructure, with the exception of mechanisms required for either the deployment or the creation of these applications and which are mainly setting configuration for their hosting and execution.

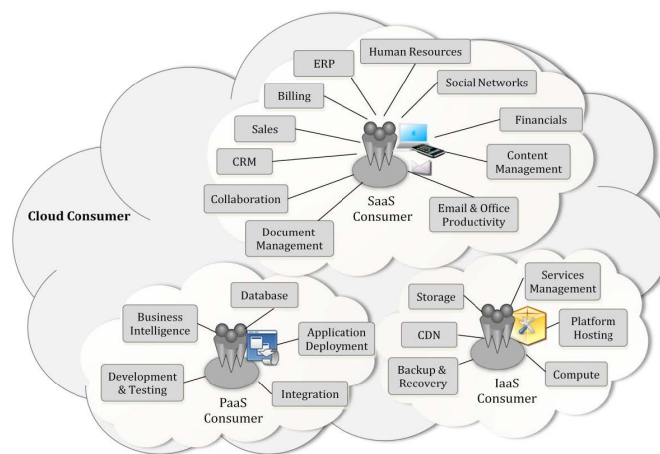


Figure 2.1. Cloud Computing service models (M. L. Badger et al., 2012).

Finally, in the last service model ([IaaS](#)), the consumer is provided with the capability to provision computing resources (VM, storage, network bandwidth), to deploy arbitrary applications and even operating systems. However, even in this instance, the consumer does not have control on the provider infrastructure, but is given mechanisms to control the deployed resources and in some cases a limited access to some selected network components such as firewalls and hosts.

If the service models determine what a consumer has access to on the provider's infrastructure, the deployment models on the other hand determine how the provider's infrastructure is deployed, who owns, operates, manages, and controls it.

The first deployment model is the "Public" one. In this instance, the provider's infrastructure is provisioned for the usage of a general public, it is owned, controlled, managed and operated by a business, government organisation, academics, etc. And is on the premise of the cloud provider.

Contrary to the first deployment model, the “*Private*” deployment model, the infrastructure is provisioned for the exclusive usage of a single organisation. However, the infrastructure may be owned, controlled, managed and operated by the stated organisation, a third party, or a combination of both, and may exist on (or off) the premise of the organisation.

In the third model referred by “*Community*”, the infrastructure is provisioned for the exclusive usage of a community —customers of organisations that share the same concerns—, and is owned, controlled, managed, and operated by a single (or multiple) member(s) of the community, a third party, or a combination of them. Similarly to the previous deployment model, the infrastructure in this instance, may be on (off) premise.

Finally, the last model “*Hybrid*” is the combination of two or more cloud infrastructures (private, public, and community). Note that even if combined, each infrastructure remains unique, and the combination is granted by the usage of standardized technologies that enable data and application portability.

M. L. Badger et al., 2012 provide an in-depth analysis of the above deployment models. The following section provides insights on the CC architectures.

2.3 ARCHITECTURE

As for the CC definitions, many researchers and organisation have proposed architectures, such as those provided by Tsai, Sun, and Balasooriya, 2010 and *Information technology — Cloud computing — Reference architecture* 2014. However, the one that gained notoriety and consensus is the one proposed by Liu et al., 2011 (see Figure. 2.2).

Among the most important aspects of the reference architecture is the introduction of five cloud actors: Provider, Consumer, Broker, Carrier, and Auditor.

As hinted in the previous sections, a Cloud Service Consumer (CSC) is a person or an organisation that maintains a business relationship with a Cloud Service Provider (CSP) for the provided service. The abiding statement of this business relationship are included in contractual agreements referred to as Service Level Agreement (SLA).

The Cloud Service Provider is an entity (person or organisation) that is providing a service to the interested parties. Therefore, a CSP is responsible for managing the infrastructure, running the associated software (in case of an SaaS delivery model), and ensures the service’s delivery through a network access. Even if the CSP responsibilities depend on the service models, its activities span across five major areas which are service deployment, service orchestration, service management, security, and privacy.

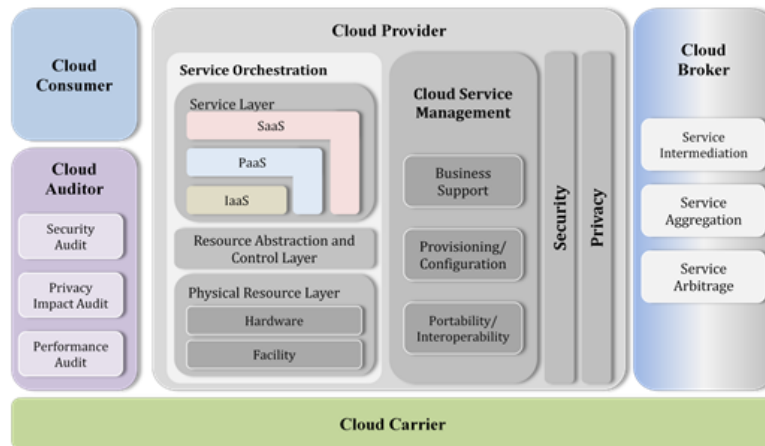


Figure 2.2. NIST Cloud Computing reference architecture (Liu et al., 2011).

A Cloud Broker (CB) is an entity (person or organisation) that manages the use, performance, and delivery of a cloud service to a CSC and negotiates the business relationship between these parties. Moreover, in some instances, a CSC may require a composite service that is provided by multiple CSPs, in this case a CB may stand as an intermediate between these providers and the CSC. Furthermore, L. Badger et al., 2014 state that a CB's main activities are: services intermediation, services aggregation, and services arbitrage.

The fourth entity described in this architecture is the Cloud Auditor (CA) that has the ability to perform an independent examination of the provided service and express an opinion. Conducted audits are done with the purpose to confirm a CSP compliance to some standards. Moreover, CA opinion must be expressed on the basis of objective evidence. Finally, expected audit areas may include service delivery, security, privacy and performance.

The last defined actor is the Cloud Carrier (CR) which is an entity that serves as an intermediary in the delivery of a service between a CSP and a CSC. More precisely, a CR ensures the connectivity and the transport of the service. Therefore, a CR provides access to the associated parties through networks, telecommunication, and other access devices.

2.4 SUMMARY

In this chapter, we provided a brief summary of CC. Indeed, there may be aspects of this paradigm that we probably did not cover in this chapter. However, we stated the main elements, such as a summary of its origins, associated definition, architecture and actors. In addition to the most cited adoption factors and opportunities, we also presented some of the most cited CC challenges.

The next chapter is dedicated to the presentation of the Digital Forensics (DF) science, its history, models, processes and standard.

DIGITAL FORENSICS

3.1	Introduction	10
3.2	Digital Forensics	10
3.2.1	Overview & History	10
3.2.2	Definitions	12
3.2.3	Investigation Models	13
3.3	Digital Forensic Readiness	17
3.3.1	Definitions	17
3.3.2	Processes and Models	18
3.3.3	DFR standards	20
3.4	Summary	23

3.1 INTRODUCTION

This chapter is dedicated to Digital Forensics (DF) science. Origins of this science, overview and definitions are provided. Additionally, this chapter contains elements about Digital Forensic Readiness (DFR), its definition, a literature overview on its associated processes, models and standards.

3.2 DIGITAL FORENSICS

Digital Forensics is a science that aims to apply scientifically proven methods to the investigation of computer related crimes. Its evolution is hence tightly related to the evolution of Information Technology (IT). In the following, we start with an overview of this science and a brief summary of its history, then we provide a set of definitions of its associated terminology.

3.2.1 *Overview & History*

Pollitt, 2010 and Roussev, 2016 tried in their works to provide a chronology that relates the evolution of this science. First, Pollitt, 2010 states 4 major phases in DF evolution, which are: Prehistory, Infancy, childhood and adolescence.

The DF Pre-history period covers the era before 1985 and is the least documented epoch. From 1960 to 1985, computer usage was primarily in industries, corporates and universities.

The first reference to “*crime with computer*” was hinted at in a book by Donn B Parker and D. Parker, 1976.

Ad hoc teams mainly composed of mainframe trained agents were formed in the US by the FBI, their sole task was to help investigators in obtaining information from the mainframe, such as data and log access. The second epoch of DF evolution is ignited by the emergence of “Personal Computers”. One of the significant events in this period was the first international Conference on Computer Evidence in 1993 held at the FBI Academy. The author states that most of the investigated cases in this period were related to fraud and the focus was mainly on recovering data from personal computers. Back then, the most used tools were home grown command line. As for the examination during this period, the investigators were forced to examine evidence on their desk or home basement. The concept of (purpose built) laboratories was not yet established, and the training that was almost rare and only provided by some associations or larger law enforcement agencies.

Pollitt, 2010 describes the period from 1995 to 2005 as being the childhood of DF. During this decade, the author notice the increase in DF maturity which was caused by several elements, such as the emergence of the Internet and the explosion in crime related to child abuse. Additionally, the author states that September 2001 event had a huge impact of the field as the terrorist in conflict region also used computer to plan their attacks or to propagate their propaganda. In regards to DF teams formation and training, the author notes the evolution in the selection of DF practitioners. Moreover, divergence in this discipline emerged due to the appearance of new devices “mobile” and “cellphone”. Furthermore, in this epoch, DF began to be driven by government agencies and professional organisation rather than by individuals. The formalisation of DF made great steps through conferences such as *the Working Group on Digital Evidence* (SWGDE).

From 2005 to 2010, the author notes: (1) the evolution in the legal venues of DF, (2) the emergence of technological advances, such as “e-discovery”, and (3) new challenges related to the volume of processed digital evidence. Moreover, DF gained recognition from IT and security professionals, and DF practitioners required academic preparation in addition to formal training. Furthermore, used tools have been updated to handle network environments, and the emergence of virtualized laboratories using dedicated forensic virtual machines. Among the events that characterise this epoch is the fact that law enforcement, military and intelligence community have designed organisational structures and processes to support their mission.

Finally, as for the future, Pollitt, 2010 predicted that: (a) attackers will be more funded, organised and educated, (b) Everyone will be at risk at all times. The author suggest some recommendations, such as: (1) DF tools must evolve and have to be automated, (2) organisations that employ DF practitioners must evolve as well through accreditation, quality management, and individual certification, (3) organisations need to cooperated in order to support the interoperability of people, tools, and processes, and (4) legal standards must evolve.

Roussev, 2016 adopted the same approach as Pollitt, 2010 and identified 3 major epochs in DF history, and which are: (1) early years (from 1984 to 1996), (2) Golden ages (from 1997 to 2007), and finally Present (2007 till now). Even if the dates are slightly different, the authors

seem to use the same approach and introduce relatively the same events. Actually, Roussev, 2016 contribution was more technical centred than the one made by Pollitt, 2010, which, for its part, is more detailed and provides the reader with more insight on the early moments of DF science.

Definitions of recurrent terms used in DF science are given in the following subsection.

3.2.2 Definitions

Some definitions which are related to : Forensics, Digital Forensics, digital evidence, digital investigation and chain of custody are given hereafter.

First, the term “Forensic” *“means a characteristic of evidence that satisfies its suitability for admission as fact and its ability to persuade based upon proof (or high statistical confidence)”* (Casey, 2011). However it may also be associated with *“The use or application of scientific knowledge to a point of law, especially as it applies to the investigation of crime”* (SWGDE and SWGIT Digital & Multimedia Evidence Glossary 2011).

As for the term “Digital Forensics” there are several definitions in the literature. For instance, it is defined as *“The use of scientifically derived and proven methods for the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations”* (Palmer et al., 2001), and as *“the application of science and engineering to the legal problem of digital evidence. It is a synthesis of science and law. At one extreme is the pure science of ones and zeros. At this level, the laws of physics and mathematics rule. At the other extreme, is the courtroom.”* (Pollitt, 1995). However, the first one seems to gain more consensus.

Digital evidence definitions are also multiple but tend to point to one key characteristic which is its admissibility in a court of justice. One of those definitions that is gaining consensus is due to (Casey, 2011), who describe it as *“any data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator”*. Moreover, digital evidence exists in two forms; “non-volatile data” (i.e., data that persists even after the computer is powered down)— and “volatile data” —(i.e., Data on a live system that is lost after a computer is powered down). The required properties of a digital evidence are: (1) Soundness, (2) Authentication, (3) Chain of Custody, (4) Integrity, (5) Objectivity, (6) Repeatability.

Digital forensic investigation (DFI) refer to the process of applying science to obtain probative evidence, it is formally expressed as *“a process that uses science and technology to examine digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred”* by (Carrier and Spafford, 2004).

Finally, the term “Chain of custody” refers to the fact that a collected or acquired digital evidence has not been tainted during the process of acquisition (or collection) or any step of the investigation. Casey, 2011 states that *“One of the most important aspects of authentication is maintaining and documenting the chain of custody (a.k.a. Continuity of possession) of evidence. Each*

person who handled evidence may be required to testify that the evidence presented in court is the same as when it was processed during the investigation”.

The following section provides some details on how an investigation is carried out, and what are the key steps in a digital forensic investigation.

3.2.3 Investigation Models

An investigation is a process which is composed of multiple steps. Even if the offences, crimes and cases may differ, there are still common steps in the conduct of an investigation. In the following, we provide details on the three most cited models, which are: (1) NIST (Kent et al., 2006), (2) DFRWS (Palmer et al., 2001), and (3) Ciardhuáinand (Ciardhuáinand, 2004).

3.2.3.1 NIST Model

Kent et al., 2006 proposed an iterative DFI model that comprises four steps (see Figure. 3.1), which are:

1. **Collection.** This first activity in this step is to identify potential digital evidence sources. Afterwards, potential evidence is collected (or acquired). Note that, there may be multiple evidence sources, and that evidence may also be either volatile or non-volatile. Therefore, it is required to have: pre-established DF collection (or acquisition) plan, assess these plans, and ensure dedicated training for those who will conduct these actions.
2. **Examination.** After the collection or acquisition, the next step is the assessment and extraction of relevant information from the collected data. In this step, some technical difficulties may appear. In fact, the desired information may be either hidden by some mechanism such as compression and encryption, or even be deleted. Additionally, in some instances the volume of the examined data may be challenging (*e.g., examination of a huge log file, or searching for information in a thousand files*). Dedicated tools with relative efficiency are already at the disposition of the examiner. However, as there are multiple types of potential evidence, format, operating systems and applications, the examiner is required to sharpen his/her knowledge on those different types, examination tools and techniques.
3. **Analysis.** Once the relevant information is examined, the analyst assesses its probative value. In this task the analyst must use a methodical approach to draw his/her conclusions. Note that, the role of an analyst is not to determine the culprit or to advance argument in favour of a party or an other. But to adopt a scientific proven method that ensures the repeatability of the analysis process. For this purpose, the analysis start by establishing hypothesis on questions (“Who, When, Why, Where, How”) related to the event or to elements associated with the event, or related to the event. To ensure the repeatability of his/her actions, an analyst should document each step and action.

4. **Reporting.** Finally, in this step, information resulting from the analysis phase is prepared and presented. Note that, there are at least three factors that may impact the produced reports. First, It is required that a report includes alternative explanations. More precisely, an analysis may also consider alternative responses or explanations in case of incompleteness (*i.e., the information about the considered event is incomplete*). The analyst may draw one or several hypotheses considering an event, and therefore analyse and explain each one of them. Second, depending to whom the reports are destined, the analyst must determine the level of details to include and how to present the result. For example, if the law enforcement are involved then the report must contain all the details and presented in a way to show the technical aspect of the adopted method. However, if the analyst is about to present his/her findings in a court of justice, the jury may not be aware of the technical aspects and may not be bothered with details that they can not understand. Finally, the third factor, is that the report must contain actionable information that may lead to the discovery of new information pertinent to the case.

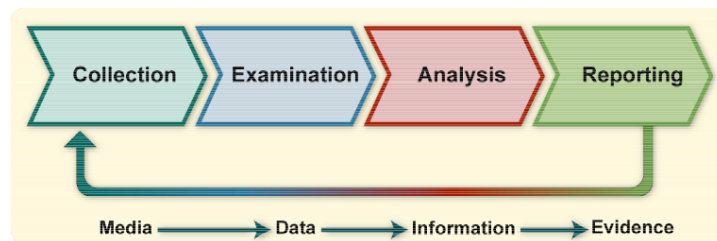


Figure 3.1. NIST Digital Forensic Investigation model (Kent et al., 2006).

3.2.3.2 DFRWS model

In the second model, Palmer et al., 2001 describe a DFI as a linear process that goes from the “Identification” to the “Decision”. As shown in Figure. 3.2, the column represent the steps of the DFI process, while the lines represent the major categories, or classes, of actions to take during a specified step. For example, during the *identification* step, actions such as event/crime detection, resolving signature, system monitoring are among the tasks to consider. Note that, the authors that in some cases, the lines may represent candidates methods or techniques to be used during the associated DFI step.

Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signature	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
Etc.		Data Reduction		Spacial		
		Recovery Techniques				

Figure 3.2. NIST Digital Forensic Investigation model (Palmer et al., 2001).

The above cited DFI process (as shown in Figure. 3.2) seems pretty straightforward. However, the authors note that only the grey coloured lines are subject to the least confusion, and that there is still a debate on the use of the term *Collection and preservation*.

In summary, Palmer et al., 2001 proposition may be considered as one of the earliest works on DFI process and models. Despite the fact that it does not contain a clear enumeration of tasks (methods/techniques) of each step, it still contains the principal steps of a DFI process that were later included in more advanced, and mature, models such as the one proposed by Kent et al., 2006.

3.2.3.3 Ciardhuáin and model

The third DFI model was proposed by Ciardhuáin and, 2004. As shown in Figure. 3.3, this model relies mainly on *Information, Information Flow, Entity, and Activity*.

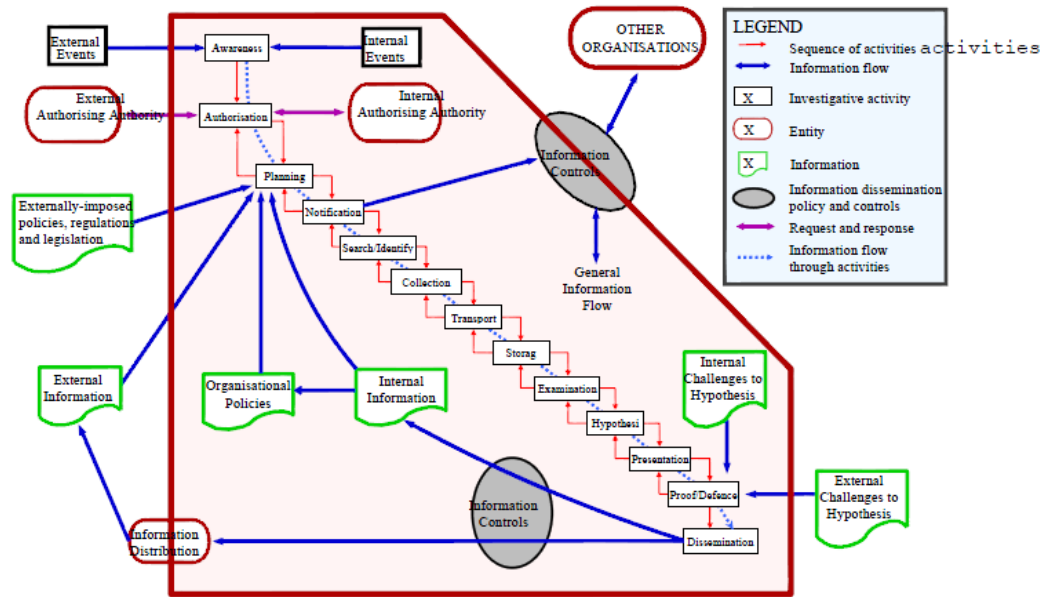


Figure 3.3. Ciardhuái Digital Forensic Investigation model (Ciardhuáinand, 2004).

Among the main characteristics of this model we may cite:

1. **Boundaries.** The proposed model makes a clear specification of the organisation (or crime scene) *boundaries*, both on term of information and control. Indeed, as shown in Figure. 3.3, the importance of boundaries is highlighted as follow: (1) the abnormal event to be investigated may be internal (or external), (2) during the investigation an authorization may be requested from an internal (or external) authority, and (3) the origins of a pertinent information related to the investigated case may be internal (or external).
2. **Activities.** The proposed model contains thirteen activities making it the most exhaustive model in term of enumerated activities (steps). Moreover, the backward chaining between each adjacent activities induces both iteration and recursion to the DFI process.
3. **Entities.** The proposed model specifies three entities responsible for : (1) authorization (internal and external), (2) information distribution, and (3) other organisation. In fact during a DFI, there may be a need to communicate with a third party, such as business partners, law enforcement, external assistance, etc. As for the information distribution, Rowlingson, 2004 has also pointed out the need to a *point of contact* who will communicate with external entities (business partner, law enforcement, external assistance) during an investigation, and also stressed the requirement of availability of such a role.
4. **Information.** Pertinent information to the investigated event may be internal or external. Moreover, for the *planning phase* (readiness), details on how this activity is done are

extracted from two sources: (1) internal, and organisational policies, and (2) external imposed policies, regulations, and legislation. Finally, in the *proof/defence* activity, the established investigation hypothesis are either challenged internally or externally.

5. **Information Flow.** As shown in Figure. 3.3, the proposed model specifies the information flow between: (1) an organisation and an external entity, (2) among the various activities, and (3) between the involved entities. Note that, this information flow is regulated by the information dissemination policy and controls.

In summary, even if Ciardhuáinand, 2004 model seems promising and do sketch how a DFI is done at some extent in an organisation, it is still not easily adaptable to other environments, especially in case of open boundaries ones. For example, in the case of CC based systems boundaries are not clear. Moreover, due to the multiples partners and tenants in a CC based system, it is not easy to trace in a precise manner the *information flow* of an abnormal event. Furthermore, even when such *information flow* is traceable, access to evidence in a multi-jurisdictions environment is challenging.

Finally, as shown in Kent et al., 2006; Palmer et al., 2001, and Ciardhuáinand, 2004 models, there must be some plan for evidence collection before the proper investigation. In fact, such plans are part of a preparedness, or readiness, phase that may shape the outcomes of an investigation. The readiness, or preparedness, of an organisation or a system to maximise the inherent ability to produce admissible digital evidence is a hot topic in DF and is commonly referred to by DFR.

The following section, provides details more insights on a this crucial phase.

3.3 DIGITAL FORENSIC READINESS

As stated in the previous sections, DFR is important during the conduct of DFI. Hereafter, we provide some associated definitions, proposed models, and processes. Finally conclude with a description ISO/IEC/27043/2015 standard (*Information technology — Security techniques — Incident investigation principles and processes* 2015).

3.3.1 Definitions

The term “*Digital Forensic Readiness*” was coined by Tan, 2001 while commenting on the results of an experiment made by the honeypot-project ¹. Tan, 2001 states that “*On average, 2 hours of intruder time turned out to mean 40 billable hours of forensic identification*”. The author then stresses the need to empower an organisation or a system with capabilities that ease the collection of digital evidence while minimising the cost of an investigation.

¹ <https://www.projecthoneypot.org/>

Moreover, Tan, 2001 defines DFR by stating that: *“Forensic Readiness has two objectives: 1)Maximizing the usefulness of incident evidence data 2)Minimizing the cost of forensics during an incident response”*.

Afterwards, many researchers provided other definitions — that while they differ in the formulation– do still keep the expressed equilibrium of maximising the ability to collect digital evidence while minimising the cost of an investigation. Among these definitions, the one provided by Rowlingson, 2004 and which states that DFR is *“The ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation”*. In the same vein Endicott-Popovsky, Frincke, and Taylor, 2007 state it as: *“maximizing the ability of an environment to collect credible digital evidence while minimizing the cost of an incident response”*.

Finally, it is important to note that there is a difference between security and DFR. Indeed, DFR is assumed on pre-established security measures. Rowlingson, 2004 states clearly that *“The assumption is made that appropriate defensive (preventative) security measures are in place in accordance with a risk assessment and that the risk assessment has sufficient information to understand the risks to the organisation from incidents where digital evidence may be required”*. Later, Dilijonaite, 2017 explained in a precise manner the difference between DFR, security and incident response.

The next subsection describes some of the most proposed models and processes that aim toward the enhancement of an organisation’s (or system’s) DFR capabilities.

3.3.2 Processes and Models

Tan, 2001 was the first researcher to both propose a DFR definition and provide a set of recommendations to strengthen an organisation (system) ability to collect admissible evidence. More precisely, the author proposed a set of technical capabilities, such as centralised logging mechanism, intrusion detection system, forensic acquisition tools and capabilities that preserve the chain of custody. Later, in 2004, Rowlingson, 2004 made a breakthrough contribution that mapped the required DFR efforts into a process that contains ten steps which are:

1. **Scenarios definition.** The first step consists in the identification of all the scenarios where the use of digital evidence is required. Therefore, it is rational to look after the risks and their impact on the organisation (or system). Threats, risks assessment and analysis should be done in order to have a clear view of what may happen. These scenarios may include situations of response to incidents and compliance to regulation and laws.
2. **Potential evidence source.** Upon the specification of potential scenarios where the usage of digital evidence is required, the next step considers the inventory of all the potential digital evidence sources. An evidence may be found at each layer of the infrastructure going from the physical level to the application one, and from sources, such as equipment, application software, monitoring solution, logs, backup and archives, etc. The author even enumerated a list of questions that may help to identify a potential source of evidence.
3. **Evidence collection requirement.** At this point, it is possible to determine from which evidence source (step 2) an evidence could help to resolve a dispute or a crime that may

occur in one of the scenarios established in step 1. However, the evidence source may be out of the control of those who may lead the investigation. Therefore, an agreement between those who are in charge of the investigation and the ones who are responsible for running and managing these evidence sources is required. Through such a statement (agreement) and in case of an investigation, a forensic investigator may state a requirement to evidence collection to those who manage and run the source (*e.g., system administrator, IT manager*).

4. **Establish a capability for securely gathering legally admissible evidence to meet the requirement.** The stated agreement in the previous step must contain the description of the required capabilities (tools) that are essential for a secure and legal collection (acquisition) of admissible digital evidence.
5. **Evidence storage and handling policy.** Now that the sources are identified, and agreement and required collection capabilities are stated, the effective collection (or acquisition) in case of investigation may be established. However, there is still a need for specifications in regards to two concerns, which are storage and handling. Indeed, digital evidence must be stored in a secure manner, and handled in a way to prevent tainting. Moreover, the admissibility of digital evidence must be secured along the pathway from the collection (acquisition) to the presentation at a court of justice. Therefore, there is a need for an established policy that dictates how evidence is handled and stored.
6. **Monitoring.** Organisation's critical assets (or a system critical modules) must be under targeted surveillance and monitoring. A rigorous risk analysis and assessment may help identify potential threats and targeted parts of an organisation's information system. The detection of a major incident leads generally to the enactment of a response —to incident— plan. However, in some instances an escalation to a full digital forensic investigation may be necessary.
7. **Escalation circumstances.** As stated in the previous point, an escalation to a full DFI is required in some instances. However, the circumstance under which such action is enacted must be specified a priori. This may be done through the review of the established scenarios in step 1. Additionally, the author states in his contribution some of these circumstances. Once the circumstances are identified, an escalation policy is established. Such policy must contain the information about the crisis manager, and point of contact that must be available on 24*7 basis.
8. **Training.** All the efforts stated in the previous points will be vain if the involved elements do not have the required training. Indeed, those who monitor must be alert to detect events that may lead to an investigation, the ones that are in charge of collecting the evidence must be able to perform their actions without tainting the evidence, and finally those who are responsible for the digital evidence examination and analysis must have the required expertise and knowledge, and be in touch with the advances in digital forensic field.

9. **Documentation.** One of the most important factors in ensuring the soundness of a DFI process is “*Repeatability*”. However, this purpose can not be achieved without proper documentation. Indeed, a systematic documentation of each taken action during an investigation ensures both the soundness of the process, its repeatability, and the maintenance of the chain of custody. Additionally, a well documented incident case may strengthen an organisation’s memory and helps the involved elements—in either incident response or DFI—to gain more knowledge from past incident when dealing with an abnormal event.
10. **Legal review.** Each action that is taken during an investigation must comply with the abiding laws and regulations. Therefore, a continuous legal review may help in establishing or asserting the legality of a collected evidence, investigation processes, and any made decisions.

While Rowlingson, 2004 provided a major contribution to the DFR field, other researchers have also investigated the required preparedness efforts in other contexts rather than an organisation. For example, Endicott-Popovsky, Frincke, and Taylor, 2007 provided an organisational framework for network forensic readiness. Furthermore, there is a breakthrough contribution that is impulsing a shift in DFR, which is referred to by Forensic-by-design, and is due to Rahman, Glisson, et al., 2016. Details on this new strategy will be provided in Chapter 5.

Finally, another major contribution to the DFR is due to (Valjarevic and Hein Venter, 2013). In their proposition, the authors provided a harmonized process model for digital forensic investigation readiness, which was later adopted and included in the ISO/IEC standard (*Information technology — Security techniques — Incident investigation principles and processes* 2015). Details on the aforementioned standard are given in the next section.

3.3.3 DFR standards

The ISO/IEC/27043/2015 standard (*Information technology — Security techniques — Incident investigation principles and processes* 2015) includes 5 groups of processes (see Figure. 3.4); Readiness processes; Initialization processes; Acquisition processes; Investigative processes; and Concurrent processes.

Details on the aforementioned processes groups are given below. However, in the context of this study, the main focus will be set on the readiness processes group.

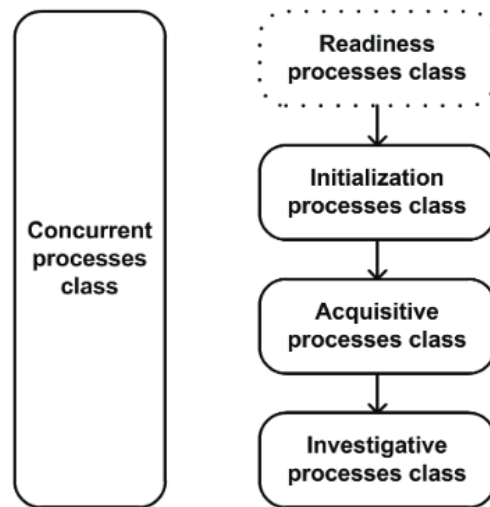


Figure 3.4. Incident investigation principles and processes groups (*Information technology — Security techniques — Incident investigation principles and processes 2015*).

3.3.3.1 Readiness

This group of processes (see Figure. 3.5) aims to ensure the due preparedness before the proper investigation and contains 3 processes groups; Planning processes group; Implementation processes group; and Assessment processes group. The first group includes activities, such as: scenarios definition (where digital evidence is required), identification of potential digital evidence sources, pre-incident gathering, potential digital evidence handling and storage, system architecture definition, etc.

3.3.3.4 *Investigative*

In case of an escalation to a full digital forensic investigation, this group contains processes that permit the acquisition, examining, analysis of digital evidence, in addition to capabilities for reports generation and investigation closure.

3.3.3.5 *Concurrent*

In addition to the forecited processes groups (i.e. readiness, initialisation, acquisition and investigation), this class of processes aims to assist during any phase of a [DFI](#) and contains processes, such as obtaining authorization, documentation, managing information flow, preserving chain of custody, preserving digital evidence, and interaction with the physical investigation.

3.4 SUMMARY

In this chapter, we provided a summarized view of digital forensic science. Going from an overview and a brief history, we, then, listed some associated definitions and investigation models.

Later, we presented the topic of digital forensic readiness. As we did for digital forensic science, we provide the reader with some details on the origins of this concept, its associated definitions, processes and models. Finally, a description of the incident investigation principles and processes standard were provided.

The following chapter is dedicated to the application of digital forensic in Cloud computing environments.

CLOUD FORENSIC

4.1	Introduction	24
4.2	Overview	24
4.3	Opportunities	25
4.4	Challenges	26
4.4.1	Systematic Literature Review	26
4.4.2	Challenges Classification	27
4.5	Cloud Forensic Readiness	30
4.5.1	Definition	31
4.5.2	CDFR Architecture	31
4.6	Summary	32

4.1 INTRODUCTION

This chapter is dedicated to the concept of “*Cloud Forensics*” (CF). First, we start with an overview of CF and its associated definitions are given, followed by a systematic literature review on its challenges. Afterwards, we introduce the concept of “*Cloud Digital Forensic Readiness*” (CDFR) along with a literature review of majors researcher’s contributions in this topic.

4.2 OVERVIEW

Cloud Forensics is the application of digital forensics in Cloud computing environments. More precisely, it was defined as being “*a cross discipline of cloud computing and digital forensics*” (Ruan, Carthy, T. Kechadi, and Crosbie, 2011). Herman et al., 2020 elaborated on the previous definition by adding that “*Technically, it consists of a hybrid forensic approach (e.g., remote, virtual, network, live, large-scale, thin-client, thick-client, including end-point devices used to access cloud services) to the discovery of digital evidence. Organizationally, it involves interactions among cloud Actors (i.e., Provider, Consumer, Broker, Carrier, Auditor) for the purpose of facilitating both internal and external investigations. Legally, it often implies multijurisdictional and multi-tenant situations*”.

Since CF is the application of DF in Cloud computing environments, then two scenarios emerge: (1) either the Cloud computing environment is considered as a crime scene to be investigated, or (2) the Cloud computing environment associated infrastructure is used to investigate a cyber-crime.

Even if the focus is more centred on the first scenario, still, there are opportunities and challenges that emerge from CF in both cases.

The next sections provide details on CF opportunities and challenges.

4.3 OPPORTUNITIES

CF opportunities come from the robustness and flexibility of Cloud computing. Ruan, Carthy, T. Kechadi, and Crosbie, 2011 identified the following:

1. **Cost effectiveness.** The implementation of forensic tools at large scale using a Cloud computing infrastructure will help in reducing the associated costs, by ensuring the availability of such tools for a large community working on several cases. Additionally, the pay per usage model of Cloud computing will help to rationalize the expenditure depending on the needs.
2. **Data abundance.** Replication and redundancy as key properties of a Cloud computing environment that may ensure secure digital evidence storage and reduce the likelihood of evidence being deleted. Indeed, the safeguard of evidence even in case of storage failure is required.
3. **Robustness.** Cloud computing storage providers offer the generation of hash and checksum on the fly ensuring the integrity of the stored data. Additionally, the IaaS model offers features such as virtual machine cloning that may benefit an investigation in several ways. For example, cloning a virtual image of an acquired evidence (disk storage, memory, network capture, etc.) may reduce the likelihood of evidence being tainted or deleted. Second such “cloning” feature may also aid in parallelizing investigation tasks such as evidence examination.
4. **Scalability & Flexibility.** Cloud computing environments are characterised by scalability on demand. Therefore, during an investigation, an examiner may allocate the required resources depending on the observed needs. For example, during a log analysis and depending on the volume of the collected log data, an examiner may opt for an Elastic search Cluster composed of multiple computation node to perform his/her tasks. The ability to allocate and liberate computing resources without a direct involvement of the provider is a key factor in ensuring that an investigator stays focused on the examined case rather than dealing with technical details.
5. **Standards & Policies.** Cloud computing being in its infancy is also an opportunity for researchers and organisations to establish policies and standards could make both Cloud computing and Cloud forensics advance hand-in-hand.
6. **Forensic as a Service.** Finally, as in the case of *Security as a Service*, forensics may be envisioned as a service. In this perspective, existent forensic tools may be exported and adapted to the Cloud computing environment, in order to establish distributed, flexible, and scalable tools for the benefit of practitioners.

4.4 CHALLENGES

Several researchers have contributed to Cloud Forensics (CF) (Herman et al., 2020; Irfan et al., 2016; Manral et al., 2020; Ruan, Carthy, T. Kechadi, and Baggili, 2013; Simou et al., 2016; Zawoad and Hasan, 2016). Efforts have been deployed either to investigate CF challenges and their classification, or to provide solutions to a single challenge or a category of challenges.

The first CF classification was proposed by Ruan, Carthy, T. Kechadi, and Crosbie, 2011 and contains three dimensions (technical, organizational, and legal). Pichan, Lazarescu, and Soh, 2015 presented a survey on CF technical challenges and proposed some solutions. For their part, Simou et al., 2016 presented a new classification based on the Cloud Forensics stages, and enumerated some proposed solutions. In their survey, Manral et al., 2020 focused mainly on solutions, artefacts identification, forensic tools, and some research gaps. More recently, Herman et al., 2020 presented the most exhaustive CF challenges enumeration (65 challenges and 9 categories). Whereas, Battistoni, Pietro, and Lombardi, 2016, focused on time synchronization and reliable timeline reconstruction. Irfan et al., 2016 presented a framework for the cloud digital evidence collection and analysis using a *Security Information and Event Management* (SEIM) tool. Zawoad, Dutta, and Hasan, 2016 worked on the cloud logging challenge, and proposed Secure-Logging-as-a-Service (SecLaaS).

In the following subsection a systematic literature review on Cloud Forensics challenges is provided.

4.4.1 Systematic Literature Review

To gain better insights on CF challenges and their classification, we have conducted a systematic literature review. For the search strategy, we have used Google Scholar and some existing databases (e.g., DBLP, ACM, IEEEExplore, and ScienceDirect) to search for existing literature, using the keyword “*Cloud Forensic challenges*” (see Table. 4.1). Note that in the IEEEExplorer case, we replaced the search query to *Cloud Forensic challenges* (without quote) ¹.

The conducted search provided 172 papers. In addition to the fourteen selected papers, we have added two pertinent papers (Herman et al., 2020; Ruan, Carthy, T. Kechadi, and Crosbie, 2011) that resulted from a literature review on Cloud Forensic. Therefore, a total of 16 papers was considered (see Table. 4.2).

¹ Only few paper resulted from that search query

Search engine	Results
IEEExPlorer *	127 (106 conference papers, 8 magazine articles, 13 journal papers)
ACM	4 (2 conference papers, 1 proceeding, 1 survey)
DBLP	34 (14 journal papers, 16 conferences and workshops, 4 Informational publications)
Science direct	7 (1 Review article, 6 Research articles)
total	172
duplicated papers	2
conferences & proceedings	125
Informational publications	4
Only citations or out of context	27
Considered papers	14

Table 4.1. Cloud Forensic challenges search results.

The excluded papers from our analysis were either duplicated papers, editorials, book chapters, or posters. However, after reading the papers, some other ones were also excluded for either having only cited CF in the literature review, or being out of the context of this study. Moreover, conference papers were also excluded as we aimed to select only papers related to CF challenges classification.

4.4.2 Challenges Classification

After the analysis of the selected papers, we note that there are three type of papers, and three categories of CF challenges classification (C₁, C₂, and C₃) (see Table. 4.2). As for the paper types, they are labelled as fellows: (T₁) Paper addressing a single CF challenge; (T₂) Papers addressing a single category of challenges; and (T₃) paper addressing multiple categories of CF challenges. For the categories, selected papers consider CF classification based on one of the following criteria: (C₁) Classification based on DFI process activities, (C₂) Classification based on the Cloud computing reference architecture, and (C₃) Other Miscellaneous classification criteria.

Reference	Type	Criteria	Categories	Challenges
Awuson-David et al., 2021	T2	C1	1	5
Choo, 2014	T2	C2	1	15
A. Cohen and Nissim, 2018	T1	C1	1	1
Alex and Kishore, 2017	T3	C2	7	15
Faheem, M. T. Kechadi, and Le-Khac, 2015	T3	C1	3	6
Grispos, Storer, and Glisson, 2012	T3	C1	4	15
Lallie, 2012	T3	C3	4	9
Lopez, Moon, and Park, 2016	T3	C1	8	20
Manral et al., 2020	T3	C1	5	25
Pichan, Lazarescu, and Soh, 2015	T2	C1	4	24
Pichan, Lazarescu, and Soh, 2018	T2	C1	1	1
Qi et al., 2017	T1	C1	1	2
Simou et al., 2016	T3	C1	4	20
Karagiannis and Vergidis, 2021	T2	C1	4	6
Herman et al., 2020	T3	C2	9	65
Ruan, Carthy, T. Kechadi, and Crosbie, 2011	T3	C3	3	9

Table 4.2. Cloud Forensic challenges selected papers comparison.

From Table. 4.2, we also observe that the most exhaustive CF classification was done by Herman et al., 2020 with 65 challenges and 9 categories (see Table. 4.3).

CF challenges
Analysis challenges
<i>Evidence correlation</i>
Reconstructing virtual storage
<i>Timestamps synchronization</i>
Log format unification
Use of metadata
Log capture

CF challenges (*Continued*)

Architectural challenges

Deletion in the cloud
 Recovering overwritten data
 Interoperability issues among providers
 Single points of failure
 No single point of failure for criminals
 Detection of the malicious act
Criminals access to low cost computing power
Real-time investigation intelligence
 Malicious code may circumvent VM isolation methods
 Errors in Cloud management
 portal configurations
 Multiple venues and geo-locations
Lack of transparency
Criminals can hide in cloud
 Cloud confiscation and resource seizure
 Potential evidence segregation
Boundaries
 Secure provenance
Data chain of custody

Legal challenges

Missing terms in contract or SLA
Limited investigative power
 Reliance on cloud providers
 Physical data location
 Port protection
 Transfer protocol
 E-discovery
 Lack of international agreements
 International cloud services
Jurisdiction
 International communication
 Confidentiality and PII
 Reputation fate sharing

Data collection challenges

Decreased access and data control
 Dynamic storage
Chain of dependencies
 Locating evidence
 Data location
 Imaging and isolating data
 Data available for a limited time
 Locating storage media
 Evidence identification
 Live forensics
 Resources abstraction
 Application details are unavailable

Data collection challenges (<i>Continued</i>)
Additional evidence collection
Imaging the cloud
Selective data acquisition
Cryptographic key management
<i>Ambiguous trust boundaries</i>
Data integrity and evidence preservation
Root of trust
Role management challenges
Identifying account owner
<i>Fictitious identities</i>
Decoupling user credentials
physical location
Authentication and access control
Standards challenges
<i>Testability, validation, and scientific principles not addressed</i>
<i>Lack of standard processes and models</i>
Training challenges
Cloud training for investigators
<i>Limited knowledge of logs and records</i>

Table 4.3. Cloud Forensics challenges classification (Herman et al., 2020).

An in-depth analysis of CF challenges is provided in Chapter 6. The following section provides insights on DFR in Cloud computing environments.

4.5 CLOUD FORENSIC READINESS

Similarly to CF being the application of digital forensics in the Cloud computing environment, Cloud Digital Forensic Readiness (CDFR) is the application of DFR in those environments. One of the earliest works in CDFR was from Ruan and Carthy, 2013b. The authors specified a set of proactive capabilities inside a Cloud Forensic Investigative Architecture (CFIA). De Marco, M.-T. Kechadi, and Ferrucci, 2014 formulated a detailed definition of CDFR and proposed a reference architecture for Cloud Forensic Readiness System (CFRS); Some of the major contributions in this topic were provided by Kebande and H.S. Venter, 2015; Trenwith and H.S. Venter, 2013, and Kebande and H. S. Venter, 2017. More specifically, Trenwith and H.S. Venter, 2013 introduced a proof of concept tool for centralized Cloud logs; Kebande and H.S. Venter, 2015 added event reconstruction into a CDFR model, and then proposed a Cloud Forensic Readiness as a Service (CFRaaS) based on a non-malicious botnet.

4.5.1 Definition

Ruan and Carthy, 2013b were the first to introduce DFR in CC environments. The authors describe it by stating that “Pro-active data collection capability is the ability of a cloud entity to maximize its potential to use digital evidence while minimizing the cost of an investigation, i.e., the preparedness and readiness of a cloud entity before an investigation”. Later, De Marco, M.-T. Kechadi, and Ferrucci, 2014 provided a more precise and detailed manner and stated it as “an Information System implemented into another system architecture with the aim of collecting and monitoring sensitive and critical information related to digital crimes before they happen, leading to save time and money for the investigations. The data is closely related to the system artifacts and logging tools available at the moment. The data is then encrypted in order to guarantee more protection and, eventually, stored on a third party server that will act as a safe, only accessible to selected subject”.

4.5.2 CDFR Architecture

There are multiple propositions that aim to ensure the DFR in CC environments, such as KEBande and H. S. Venter, 2017; KEBande and H.S. Venter, 2015; Trenwith and H.S. Venter, 2013. We, however, will focus on the one proposed by De Marco, M.-T. Kechadi, and Ferrucci, 2014, as it is more abstract and aims to be a reference architecture (see Fig. 4.1).

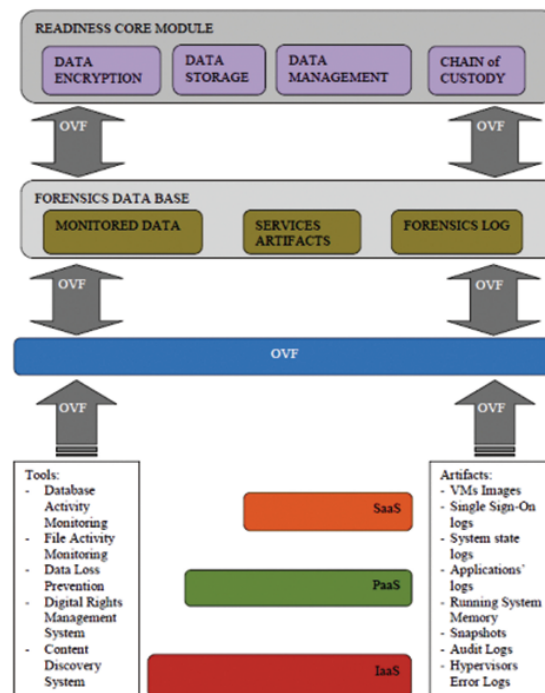


Figure 4.1. CFRS reference architecture (De Marco, M.-T. Kechadi, and Ferrucci, 2014).

The above cited architecture stands mainly on the Open Virtualization Format (OVF) standard. The DMTF defines OVF as an “open, secure, efficient and extensible 229 format for the packaging and distribution of software to be run in virtual systems” (DMTF, 2015).

De Marco, M.-T. Kechadi, and Ferrucci, 2014 propose in their architecture the usage of OVF as a transport medium for digital evidence. In fact, in their architecture, digital evidence are extracted from multiple artefacts, such as logs, system’s states, snapshots, etc. which are scattered along the targeted Cloud infrastructure —depending on the associated service model (IaaS, PaaS, or SaaS)— with the aid of associated digital forensic tools. Once the digital evidence are extracted, they are stored in the digital evidence database depending on their nature (monitoring logs, artefacts, or forensic logs). Finally, as a supervision capability, the core readiness module includes components that ease some tasks such as those related to the encryption, storage, management, and the chain of custody maintenance.

Note that, even if the proposed architecture seems promising, it is still not yet implemented. As far as we know there is still no concrete solution that ensures the due DFR in CC environments.

Additionally, in regards to De Marco, M.-T. Kechadi, and Ferrucci, 2014 proposition, relaying on the OVF has its advantages as it has its limits too. In fact, the main insufficiency from which the proposed architecture suffers is the fact that it does not consider other forms of virtualization such as the OS level one.

4.6 SUMMARY

In this chapter we provided a summarized view of “Cloud Forensics”. Going from an overview and definitions to associated opportunities and challenges. CF challenges are divers and dependants. Moreover, there are multiple classifications. Therefore, a systematic literature review was conducted to determine CF challenges and how researchers tend to classify them.

Later, we presented the topic of “Cloud Digital Forensic Readiness”. As we did for the CF, we took time to provide the reader with some details on the origin of this concept, and its associated definitions. While, the propositions that aim to enhance a CC with the due DFR capabilities are multiple, we preferred to focus on the most promising one, which is the Cloud Forensic Readiness System (CFRS).

The next chapter is dedicated to the introduction of a new paradigm that is “Forensic-by-Design” (FbD) that may induce a new vision in enabling systems with the due DFR capabilities.

5.1	Introduction	33
5.2	Systematic Literature Review	33
5.3	FbD Frameworks	38
5.4	Opportunities and Challenges	40
5.4.1	Opportunities	40
5.4.2	Challenges	44
5.5	Research Gaps	47
5.6	Hypothesis	47
5.7	Summary	48

5.1 INTRODUCTION

In this chapter, we will introduce an emerging concept which is Forensic-by-Design (FbD) (Rahman, Glisson, et al., 2016). Similar to Security-by-Design (SbD), this new paradigm extends DFR perspectives. More precisely, FbD advocates the integration of forensic requirements into the earliest phases of a system's design and development stages, in addition to a continuous monitoring of the system's *forensic-ready* state.

This approach stands inevitably and implicitly on a conjugate of two disciplines (digital forensics (DF) and System & Software Engineering (SSE)), and aims towards *forensic-ready* engineered systems.

In order to bring clarity on this new strategy, we will: (1) present a systematic literature review on FbD, (2) provide details on existent FbD frameworks, (3) investigate some related challenges and opportunities, (4) identify some research gaps, and (5) make an hypothesis on FbD efficiency in the context of Cloud computing systems.

5.2 SYSTEMATIC LITERATURE REVIEW

Introduced by Rahman, Glisson, et al., 2016, FbD was first intended for Cyber-Physical Cloud Systems (CPCS). Additionally, the authors proposed an associated conceptual framework (see Fig. 5.1), which may be summarized into two pertinent aspects.

First, the proposed framework advocates the inclusion of six key factors during a system design and development stages. Those key factors are: (1) Risk management, (2) Forensic readiness, (3) Incident handling, (4) Laws & regulations, (5) CPS's Hardware and software, and

(6) Industry-specific. Second, it specifies the need for a continuous monitoring of the system's *forensic ready* state.

Many researchers have already suggested the application of FbD strategy to enhance DFR, such as Grispos, Glisson, and Choo, 2017; Le-Khac et al., 2020; Rahman, Cahyani, and Choo, 2016. However, there are still some unanswered questions, especially in the case of Cloud Computing systems. The main objective of this section is to answer the following:

1. What are the domains for which the FbD was proposed?
2. What are the proposed key factors?
3. What are the FbD provided standards and best practices?
4. What are the FbD cited challenges and open issues?

More specifically, answering the above questions will help us to: (1) establish the scope of FbD application, (2) enumerate all the cited FbD key factors in order to conduct a mapping with the CF challenges, and (3) obtain indications on the alignment of FbD and SSE standards. For the search strategy, we have used Google Scholar and some existing databases (e.g., DBLP, ACM, IEEEExplore, and ScienceDirect) to search for existing literature, using the keyword *Forensic-by-design* (see Table. 5.1).

The conducted search provided 47 papers, of which only 11 were considered for analysis (see Table. 5.1). Excluded papers from further analysis were either editorial, or papers that have only cited FbD in their literature review and papers that were considered out of the scope of this study. We have added another pertinent paper (Alenezi et al., 2017) which resulted from a literature review on Cloud Forensic Readiness (see Section. 4.5).

Search engine	Results
IEEEXPlover	4 (1 magazine article, 3 conference papers)
ACM	8 (1 editorial, 3 conference papers, 3 proceeding papers, 1 survey)
DBLP	5 (3 journal papers, 2 conference and workshop papers)
ScienceDirect	30 (5 review articles, 18 research articles, 2 book chapters, 3 editorials)
total	47
Duplicated papers	6
Editorials	4
Only citations or out of context	26
Considered papers	11
Selected papers	
Reference	Title
Rahman, Glisson, et al., 2016	Forensic-by-Design Framework for Cyber-Physical Cloud Systems
Grispos, Garcia-Galan, et al., 2017	Are you ready? Towards the engineering of forensic-ready systems
Rahman, Cahyani, and Choo, 2016	Cloud incident handling and forensic-by-design: cloud storage as a case study
Choo, Esposito, and Castiglione, 2017	Evidence and forensics in the cloud: Challenges and future research directions
Grispos, Glisson, and Choo, 2017	Medical Cyber-Physical Systems Development: A Forensics-Driven Approach
Pasquale et al., 2018	Towards forensic-ready software systems
Parra, Rad, and Choo, 2019	Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities
Le-Khac et al., 2020	Smart vehicle forensics: Challenges and case study
Malamas et al., 2019	A Forensics-by-Design Management Framework for Medical Devices Based on Blockchain
De La Torre, Rad, and Choo, 2020	Driverless vehicle security: Challenges and future research opportunities
Yaacoub et al., 2020	Cyber-physical systems security: Limitations, issues and future trends

Table 5.1. Forensic-by-design search results

Results and findings from the analysis of the selected papers are presented in Tables. 5.2 and 5.3.

Reference	Domain	Key Factors	Challenges	Best Practices & Standards
Rahman, Glisson, et al., 2016	Cyber-Physical Cloud systems	✓	–	✓
Grispos, Glisson, and Choo, 2017	Medical Cyber-Physical systems	✓	–	✓
Pasquale et al., 2018	Software systems	–	✓	–
Grispos, Garcia-Galan, et al., 2017	System Engineering	–	✓	–
Alenezi et al., 2017	Cloud Forensic Readiness	–	✓	–
Rahman, Cahyani, and Choo, 2016	Cloud computing systems	–	–	–
Choo, Esposito, and Castiglione, 2017	Cloud computing systems	–	–	–
De La Torre, Rad, and Choo, 2020	Driverless vehicle	–	–	–
Manral et al., 2020	Cloud Forensics	–	–	–
Malamas et al., 2019	Health care management systems	–	–	–
Le-Khac et al., 2020	Smart Vehicle	–	–	–
Parra, Rad, and Choo, 2019	Smart Grid & Industrial Internet of Things	–	–	–

Table 5.2. FbD selected papers comparison (part1).

Proposed FbD Key factors and their associated best practices				
Key Factor	Cited In		Best practice Proposed by	
	Rahman, Glisson, et al., 2016	Grispos, Glisson, and Choo, 2017	Rahman, Glisson, et al., 2016	Grispos, Glisson, and Choo, 2017
Risk management	✓	✓	–	–
Forensic readiness	✓	✓	ISO/IEC/27043 standard	Rowlingson, 2004
Incident handling	✓	–	Shields, Frieder, and Maloof, 2011	–
Laws	✓combined with Regulations	✓	–	–
Regulations	✓Combined with Laws	✓	PC-DSS	–
Hardware and software	✓	✓	–	–
Industry-specific	✓	–	–	–
Security	–	✓	–	Haley et al., 2008
Privacy	–	✓	–	Act, 1996
Safety	–	✓	–	–
Medical	–	✓	–	–
Cited FbD challenges and Open issues				
Pasquale et al., 2018	Representing and reasoning about Forensic-ready systems; Methods for engineering forensic-ready software systems; Verification of forensic readiness requirements; Technological developments			
Grispos, Garcia-Galan, et al., 2017	Elicitation of requirements for forensics; Stakeholder Analysis for “forensic Requirements”; Evaluating the impact of Laws and Regulations on Requirements for forensics; Forensics Trade-off Analysis; Addressing System Performance Overhead in Forensic-by-Design; Assessing the influence of Forensic-by-Design on the Forensic Readiness Ecosystem			
Alenezi et al., 2017	Architecture; SLA; Management Support; Governance; Culture; Training; and Procedures			

Table 5.3. FbD selected papers comparison (part2).

Tables 5.2 and 5.3 provide the following indications:

1. Most of the associated research papers are only citing FbD, either in the literature review, or as a perspective for future works;
2. Major considered papers feature topics from the following domains: Cyber-Physical Systems, Cloud Computing Systems, Smart Vehicles (driverless or not), Health Care Systems, System engineering, and one paper on Software systems.
3. Only three papers (Alenezi et al., 2017; Grispos, Garcia-Galan, et al., 2017; Pasquale et al., 2018) discuss the FbD challenging aspects and open issues;
4. Only two papers (Grispos, Glisson, and Choo, 2017; Rahman, Glisson, et al., 2016) made propositions of FbD key factors. However, none of them provides a clear and concise selection criteria for FbD key factors;
5. Only two papers (Grispos, Garcia-Galan, et al., 2017; Rahman, Glisson, et al., 2016) provide some best practices or standards to some of their proposed key factors.
6. There is no concrete implementation of the FbD paradigm. The only paper that seems to provide indications on a potential implementation is due to Rahman, Cahyani, and Choo, 2016 and was centered on Cloud incident handling in a Cloud storage case study, without any technical details on the implementation.

In the following we will first discuss FbD frameworks and associated key factors in Section 5.3, and then FbD related challenges and opportunities in Section 5.4.

5.3 FbD FRAMEWORKS

The first FbD (*conceptual*) framework was proposed by Rahman, Glisson, et al., 2016 as shown in Figure 5.1. This framework was intended for Cyber-Physical Cloud Systems, and its main aspects are: (1) integration of forensic requirements in the design and development stages, (2) verification and validation, and finally (3) continuous reviews of the desired state of forensic readiness.

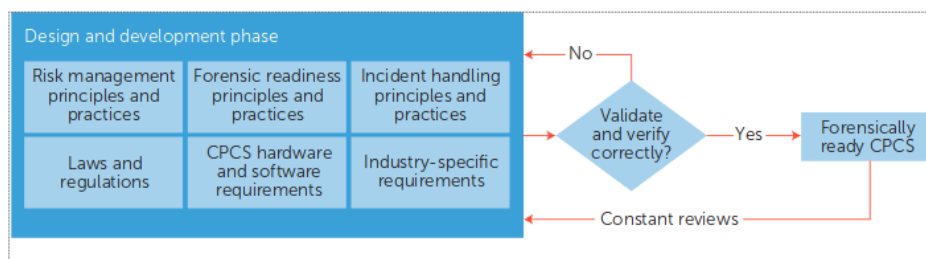


Figure 5.1. A conceptual Forensic-by-design framework (Rahman, Glisson, et al., 2016).

Even if Rahman, Glisson, et al., 2016 framework seems intuitive and encapsulates the main idea of integrating forensic requirements during the earliest phases of a system' design and development stage, there are still some unanswered questions:

1. What is the adopted criteria for key factors selection?
2. Is the desired system's *forensic-ready* state related only to the design and development stages or should it be all along the system life cycle?
3. What are the associated best practices or standards to follow in order to guarantee the integration of the stated key factors?
4. How to apply the proposed framework in case of : (1) A system composed of multiple subsystems, (2) Service composition, (3) Integration of multiple components inside a system?

The second framework was brought by Grispos, Glisson, and Choo, 2017 in the context of Medical Cyber-Physical systems as shown in Figure. 5.2. The proposed framework adopts the same concept as in Rahman, Glisson, et al., 2016 (i.e., *The integration of some key factors during the system' design and development stage, and a continuous monitoring of the resulting forensic-ready state*). However, it adopts more key factors (nine) in comparison with the first one (six).

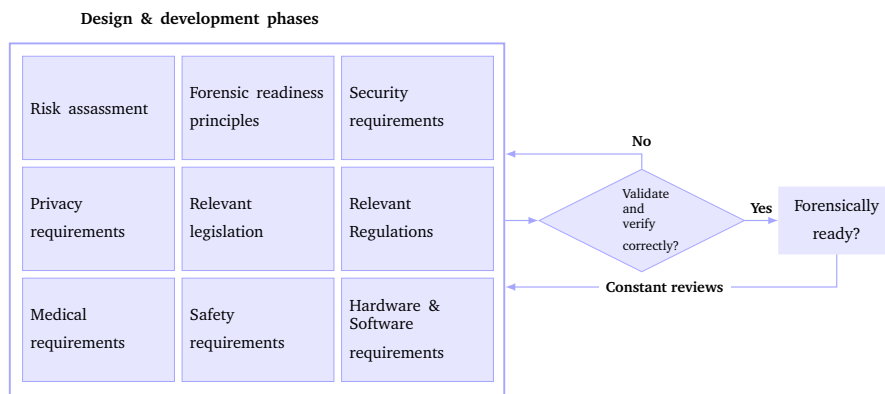


Figure 5.2. A Medical Cyber-Physical System Forensic-by-design framework (Grispos, Glisson, and Choo, 2017).

Some of the newly adopted key factors (Security, Privacy and Safety) are primarily related to the domain of application (Medical, Healthcare) rather than some more general engineering or conceptual requirements.

As stated for Rahman, Glisson, et al., 2016 framework, this second framework do not provide answers on *how* to achieve the integration of forensic requirements into a system' design and development stages, neither it answers questions on the resolve issues related to systems or

service composition, nor it provides specific standards or guideline to follow in order to achieve the integration of its stated key factors into the system's design and development.

5.4 OPPORTUNITIES AND CHALLENGES

Some researchers have already pointed out the benefit of [FbD](#), while some others have enumerated some issues and open questions. In the following, we will first address the benefits that may arise from adopting this new paradigm, then we will discuss the most cited challenges and issues.

5.4.1 Opportunities

From the previous [FbD](#) systematic literature review (see Section. [5.2](#)), it appears that this new paradigm may be used to either design and develop *forensic-ready* systems, or to help in an ongoing [DFI](#). We may categorise the advantages of this new strategy into the following: (1) Versatility, (2) Standardisation, (3) Consolidation.

5.4.1.1 Versatility

Even though the Rahman, Glisson, et al., [2016](#) framework was first intended for Cyber-Physical Cloud Systems, many researchers have already suggested the application of [FbD](#) and its associated framework—with required adjustments—in other domains. As shown in Table. [5.2](#), there are at least five other contexts that may be suitable for this new strategy.

Grispos, Glisson, and Choo, [2017](#) have already proposed a variant of the [FbD](#) framework for Medical Cyber-Physical Systems (see Fig. [5.2](#)). The authors kept some of the essential aspects of Rahman, Glisson, et al., [2016](#) framework, such as integrating a set of key factors during the design and development of a system, verification and validation of the resulting forensic-ready state and finally the continuous monitoring. However, they added three new key factors (Security, Privacy and Safety). Even if the newly added key factors were justified from the perspective of the application domain (Medical), the authors did not provide any standard or best practices to ensure a proper integration of their proposed key factors. As for validation, the authors provided a set of recommendations based on the analysis of an hypothetical case study (fusion pump).

While investigating Smart Vehicle Forensic challenges, Le-Khac et al., [2020](#) proposed the adoption of [FbD](#) in the design of future vehicles. The authors argue that the adoption of this new paradigm may facilitate the conduct of [DFI](#) in smart vehicles. The authors' motivation for the adoption of this paradigm comes from the challenging aspect of [DFI](#) in Smart Vehicles, as the authors state: "*The complexity and variety of systems in vehicles complicate forensic investigations. For example, to investigate a modern-day vehicle, the investigators may also have to understand the workings of 20 or more electronic modules, their configurations, and their interactions.*" (Le-Khac et al.,

2020, pg 502, Sec. 3, ¶5). In the same line, De La Torre, Rad, and Choo, 2020 proposed the adoption of FbD for Driverless vehicles.

Other than Smart vehicle and Medical Cyber-Physical Systems, Parra, Rad, and Choo, 2019 proposed the adoption of FbD for Smart grid systems, and Goudbeek, Choo, and Le-Khac, 2018 advocated the use of this new paradigm in a Smart Home (Home Automation Systems). A complete list of FbD potential application domains is provided in Table. 5.2.

5.4.1.2 *Standardisation*

In a discussion on CF future directions, Choo, Herman, et al., 2016 proposed the establishment of a Cloud Forensics Reference Architecture (CFRA), or a Cloud Forensic-by-Design Framework (CFbDF). Author's suggestion was in response to (Herman et al., 2020) CF challenges classification, and aims to provide a common framework or language to the different involved stakeholders (Cloud providers, consumers, auditors, carrier and brokers) to communicate with each other on CF issues, such as uses, standards, etc. However, authors state that such a solution should be independent of any offerings and technologies. Finally, among the benefits of such a solution, the authors stated the possibility to use it for CF candidate standards analysis and evaluation.

5.4.1.3 *Consolidation*

This category contains research contributions that aim towards a consolidation of existent forensic capabilities in order to facilitate a DFI or to investigate the venue of forensic-ready tools that will enhance the success of a DFI.

Rahman, Cahyani, and Choo, 2016 introduced an integrated model which incorporates Forensic-by-Design principles with existent incident handling strategies (see Figure. 5.3). More precisely, they intended to incorporate the already established (Rahman, Glisson, et al., 2016) framework key factors into an existent incident handling model. As for the incident handling model, the authors adapted an existing model that contains six iterative key phases which are:

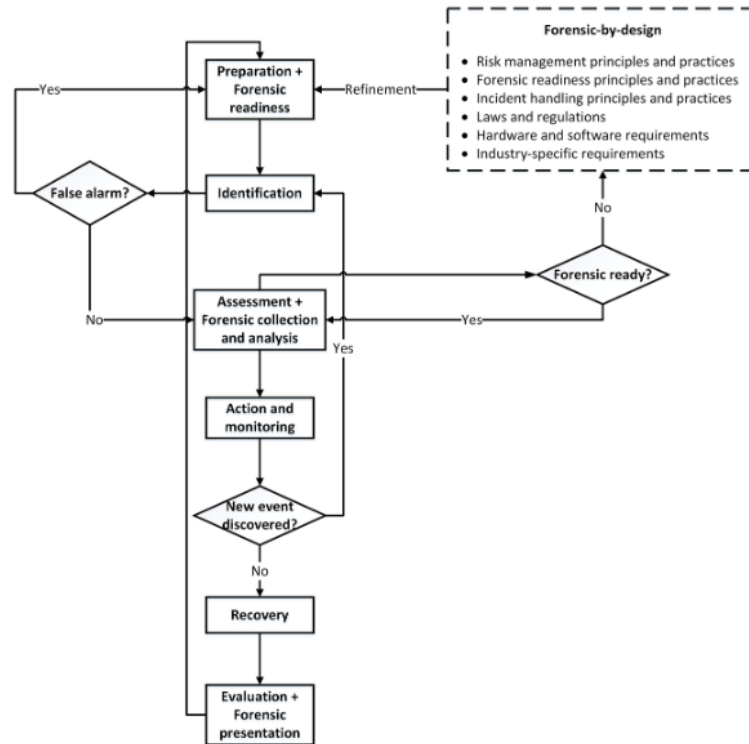


Figure 5.3. An integrated cloud incident handling and forensic-by-design model (Choo, Herman, et al., 2016).

1. **Preparation.** Contains activities aimed towards the implementation of proactive measures to protect data and prevent security incidents from occurring. The authors advise to update risks assessment in order to include and to assess emergent incident types.
2. **Identification.** Upon the detection or report of an abnormal event, it is first assessed whether it is a false negative or not. If not, then the model proceeds to assess the risk from the event and the efficiency of the existent forensic collection and analysis capabilities. Note that, if those capabilities are not “forensic-ready” then a return to the design phase is required in order to refine the preparation capabilities. This refinement is made possible through the integration of [FbD](#) key factors as stated in Rahman, Glisson, et al., 2016.
3. **Assessment.** In this phase, the authors recommend the integration of forensic collection and analysis practices. As stated by the author: “In-depth incident investigations will subsequently take place generally for high and medium incident scale (as incidents with low impact may not require in-depth investigations) to determine who, what, where, when, and how an incident took place” Rahman, Cahyani, and Choo, 2016, pg 5, Sec. 3, ¶3.
4. **Action and Monitoring.** Required actions to be taken in this phase are related to the event handling. For example, containment (i.e., prevent the event from spreading) and

eradication (*i.e.*, *eliminate the incident component*). However, those response actions should be taken after an image copy was created in order to preserve potential digital evidence. As for the monitoring, it is a continuous action that is required to both check for the occurrence of an abnormal event or the efficiency of the undertaken response action, but also a continuous verification of the system's forensic-ready state.

5. **Recovery.** This phase is concerned with the return to normal, secure and operational state. A backup plan and/or a disaster recovery strategy must be activated at this stage.
6. **Evaluation.** After the incident has been resolved, a formal evaluation is conducted to discuss issues related to: (1) incident origin and its impact, (2) efficiency of the conducted assessment, (3) effectiveness of the response, and (4) learned lessons. Therefore, a forensic representation of all the findings is established. However, forensic reporting must also emphasise the fact that many stakeholders may be unfamiliar with technical terms. Therefore, the drafting of such a report must integrate this constraint, and reports must include all the received positive and negative feedbacks from evaluation meeting.

To summarise, in the proposed model and upon identification of an incident, the forensic collection and analysis capabilities were assessed. Depending on the incident nature, the system design may be reviewed in order to ensure an up-to-date DFR. In fact, in the occurrence of a *Not yet encountered* event, the “constant reviews” (Fig. 5.3) is triggered. A proof of concept of this model based on a malicious content distribution in a cloud storage case study was also presented.

Another perspective of consolidation (*i.e.*, *Using FbD to enhance existent forensic capabilities in order to facilitate the conduct of a DFI*) was provided by Bollé, Casey, and Jacquet, 2020. In their study, the authors investigated the role of evaluation in reaching decisions using automated systems (*i.e.*, *any system that performs a process instead of a person to address forensic questions (authentication, classification, identification, reconstruction, evaluation)*).

As stated by the authors, automated systems allow forensic practitioners to perform analysis tasks that would otherwise be infeasible. Furthermore, the authors provided examples of automated systems and tasks where the usage of these systems is recommended such as Child Sexual Abuse CSA material classification to reduce forensic examiner exposure to stress. However, the usage of these systems to reach decisions —without a critical and scientifically based evaluation of these systems— may lead to undetected errors or bias resulting in wrong decisions. Therefore, the authors state that: “*In order to support decisions in a forensic setting, the design of software should abide by forensic principles and practices (Rahman, Glisson, et al., 2016).*”.

In other words, automated systems may facilitate the conduct of a DFI, however their usage must be allowed under the assumption that they are not subject to error, and that they are scientifically evaluated. Therefore, even automated systems must be forensic-ready. Even if there are many arising opportunities from the FbD paradigm, there are still some challenges and open issues. In the next subsection, we will present an overview of the FbD challenges and issues that were cited in the literature.

5.4.2 Challenges

For the FbD challenges, the systematic literature review shows three main publications Alenezi et al., 2017; Grispos, Garcia-Galan, et al., 2017; Pasquale et al., 2018 that goes more or less in the details of this new paradigm's issues. While investigating the opportunities of a conceptual framework for CDFR in organisations, Alenezi et al., 2017 identified several required factors, that they regrouped in three main categories (technical, legal and organisational).

In Alenezi et al., 2017, the technical factors represent the technological aspects that influence the DFR in the Cloud computing environment, such as Infrastructure, Architecture, Technologies, Security. As for the legal ones they include aspects related to: (1) agreements between a CSP and a CSC (SLA), and (2) abiding laws in a specific jurisdiction or multi-jurisdictions, and regulatory. Finally, the organisational factors contain some of the organisation and employees characteristics that may facilitate the CDFR, such as Management support, Strategy, Governance, Culture, Training, and Procedure.

The results of a mapping conducted by the authors involving twelve previous studies and the stated factors reveal that the framework proposed by Rahman, Glisson, et al., 2016 do not contain the following factors: Architecture (Technical), SLA (Legal), Management support, Governance, Culture, Training and procedure (Organisational).

One of the most pertinent aspects that Rahman, Glisson, et al., 2016 lacks is the *Architecture* which is described by Alenezi et al., 2017 as : *"The system architecture must be designed in a specific way so as to increase its forensics capabilities"*. Even if Rahman, Glisson, et al., 2016 framework aims towards the design of a *"forensic-ready"* system, it is still not clear *How* the proposed integration of forensic requirements in the design and development stages will lead to system with increased forensics capabilities. As the Rahman, Glisson, et al., 2016 framework answers *"What"* is required to achieve *"forensic-ready"* systems, it fails to provide answers to the *"How"* questions.

The second study on FbD opportunities and challenges was due to Grispos, Garcia-Galan, et al., 2017. In their contribution, the authors investigated the potential benefits that may arise from the adoption of FbD as an alternative strategy for DFR. While stating that this shift in DFR perspective has already been discussed in the literature, they stress the fact that there is still no previous work that discusses the extent to which organisations consider forensics requirements during systems development. Therefore, after an assessment of existing research on DFR perspectives, the authors proceeded to an online survey in order to get a clear and straightforward appreciation of this new strategy (FbD) from the system/software engineering community.

126 participants attempted Grispos, Garcia-Galan, et al., 2017 online survey and were either in the field of system/software engineering (engineer, project manager, programmers, developers) or system/software security related roles (consultant, engineer, analyst, managers, etc.). Results from this survey point out the following research challenges:

1. **Elicitation.** Lack of elicitation techniques and analysis of forensic requirements at the start of the development process.

2. **Analysis.** The design and development stages involve a variety of stakeholders participation. However, it is not yet clear how to accommodate stakeholders interests and needs for *forensic* in the system requirements definition.
3. **Law & regulation.** Potential conflicts from multi-jurisdictional laws and regulations may have an impact on the forensic requirements definition.
4. **Trade-off.** Forensic requirements potential conflicts with other requirements, such as security and privacy, imply the need to trade-off techniques and analysis.
5. **Performance.** A system performances overhead may result from the implementation of forensic requirements (eg. Intensified user activity logging and system snapshots).
6. **Influence.** Lack of assessment on the *FbD* impact on the implemented *DFR* policies and procedures.

Finally, the last study on *FbD* issues and challenges was done by Pasquale et al., 2018. Stating that “*forensic-ready*” software systems (*i.e., capable of supporting potential digital investigations*) are critical. The authors then focused on the role of *DFR* in software engineering practices. Arguing that data has a central role in providing insights on how a particular incident occurred and by whom, the authors defined *DFR* in the context of software engineering as “*a property that encapsulates the capabilities of software to: (1) conduct digital forensic processes in a forensically sound way; and (2) produce forensically sound evidence*”.

To show what motivated their research, the authors discussed a peer-to-peer (P2P) toolkit (iCOP), which is more precisely designed and conceived with the aim to identify, preserve and analyse new or previously known *CSA* media shared between suspects on peer-to-peer networks.

Afterwards, the authors proceeded to describe a set of requirements for “*forensic-ready*” software systems. The aforementioned requirements were either data-centered or process-centered, and were elicited by authors’ review of existing literature on *DFR*. The established set of requirements contains: Availability, Relevance, Minimality, Linkability, Completeness, Non-Repudiation, Data provenance, and Legal compliance. Finally, the authors state that there are four categories of challenges:

1. **Representation and reasoning.** Elements of this category are related to the conceptualisation of *DFR* requirements of software systems, and are regrouped in three subcategories: concept (*i.e., represent and reason about forensic-ready system and their proprieties*), methods (*i.e., how to design and implement forensic-ready systems*), tools (*i.e., how to analyse and support the development of forensic-ready systems*). Even if the authors did not provide details on these issues, they stressed the need to identify formal language —If any— that are best suited to express *DFR* requirements.
2. **Methods.** This category contains challenges that may arise in the process of adapting existing software/systems engineering methods to take into account the forensics readiness requirements. In this category, the authors question the nature of *DFR* as if it were solely

about data preservation activities. Moreover, they also point out the opportunity to use “*Architectural patterns*” such as security patterns into the design of forensic-ready systems. However, at the same time they warn about the necessity of requirements trade-offs that may be needed to maintain a balance between the need for digital forensic evidence and at the same time the safeguard of privacy.

3. **Verification.** Being a key step in systems/software design process, the authors ask whether it is required to either adapt the already existent verification methods —those related to security and safety verification— or there is a need for the development of new techniques. Moreover, the authors also ask whether the satisfaction of forensic readiness requirement can be satisfied (verified) at the design time. Furthermore, the authors bring the focus on the hypothetical performance overhead that may result from the integration of [DFR](#) requirements, and the need for trade-offs with other systems/software requirements.
4. **Technological development.** This category contains issues that may emerge from technological advancement (*e.g., IoT, Smart cities, Cyber-Physical Cloud Systems, wearable devices*) and their impact on systems’ design process. The authors argue that: “*In such smart cyber-physical environments, the system design cannot be anticipated a-priori and is only emergent a-posteriori when various IoT devices dynamically compose to deliver various services*”. Moreover, the authors point out the volatility of the system’s design in such cases.

In summary, from the conducted systematic literature review, there are only three papers that investigate [FbD](#) issues and challenges. All of the three cited above adopted different approaches. While Alenezi et al., [2017](#) used a three dimensionality regrouping, the authors still do not provide details on their choices nor do they explain in depth the [FbD](#) lacking aspects and issues. As for Grispos, Garcia-Galan, et al., [2017](#), the authors opted for a survey involving systems/software engineering community around potential challenges and issues. However, as in Alenezi et al., [2017](#), the authors do not investigate the origins of these issues. Finally, Pasquale et al., [2018](#) adopted an approach based on systems/software engineering methods. Afterwards, with the aid of a concrete example, they described a set of required factors and four categories of challenges that may arise in engineering forensic-ready systems. A summary of this Subsection finding is provided in Table. [5.4](#).

Reference	Approach	Challenges
Alenezi et al., 2017	3 dimensions (Technical, Organisational and Legal)	Architecture, SLA, Management support, Strategy, Governance, Culture, Training, Procedure
Grispos, Garcia-Galan, et al., 2017	Online Survey	Elicitation, Analysis, Law & regulation, Trade-off, Performance, Influence
Pasquale et al., 2018	Systems/Software engineering methods	Representation and reasoning, Methods, Verification, Technological Advancement

Table 5.4. FbD issues and challenges.

5.5 RESEARCH GAPS

As shown in the previous section, there are apparent opportunities from FbD, but at the same time there are several challenges and issues. While the opportunities seem to be categorised in three major groups, the challenges appear heterogeneous and sparse as described in Subsection. 5.4.2. Certainly, for now there are only three research studies that investigated the challenging aspects of FbD. Even so, there is no consensus on how the resulting/enumerated challenges are established. In fact, as far as we know, none of the previous works have provided answers to the following questions:

1. Why is FbD challenging?
2. What are the sources of these challenges?

More importantly, the main question to answer is the following: *Does FbD challenges imply a questioning of the whole paradigm or just its associated framework?*

Recalling that FbD paradigm is conceptually similar to SbD, with the aim to integrate forensic requirements into the design and development phases of a system's life cycle, we may derive two important questions:

1. Is the FbD paradigm feasible/suitable/efficient for any type of system?
2. Is the forensic requirements integration as aimed by FbD achieved in accordance to existent systems/software engineering standards or best practices?

We believe that Rahman, Glisson, et al., 2016 stated the FbD paradigm intuitively for system-s/software without any in-depth analysis of its inherent boundaries. Moreover, the authors introduced this new concept as an abstract one, without any indications on a potential methodology that may facilitate its implementation in real world projects. Furthermore, implying the conceptual similarities between FbD and SbD without indicating the need to associate them with the systems and software engineering domain may undermine the potential of this new concept.

Finally, in the next Section, we state an hypothesis on FbD efficiency in some types of systems.

5.6 HYPOTHESIS

After analysis of FbD challenges and opportunities, it is clear that the proposed FbD frameworks still do not answer some aspects that are either related to a system composition and structure, nor it answers questions on the alignment of this new concept with established System & Software Engineering standards and best practices.

Therefore, we come up with an hypothesis that summarizes our critics of FbD. More precisely, we hypothesize that: *(a) this new alternative is not effective for some open boundaries systems, and (b) this strategy is not fully aligned with the systems and software engineering standards.*

The proof of the formulated hypothesis, and an improved FbD are provided in the next chapter.

5.7 SUMMARY

Forensic-by-Design is a trending paradigm that offers a different perspective of Digital Forensic Readiness. As promising as it seems to be, it still presents some issues and challenges. Indeed [FbD](#) is still a fresh topic (2016–2022).

The following chapter is dedicated to the proof of the stated hypothesis (see Section. [5.6](#)) and to the proposition of an improved [FbD](#) framework.

AN IMPROVED FORENSIC-BY-DESIGN FRAMEWORK

6.1	Introduction	49
6.2	Hypothesis arguments	49
6.2.1	Key factors & Challenges Mapping	50
6.2.2	Persistent Challenges Filtering	55
6.2.3	FbD alignment with SE standards	57
6.3	The proposed framework	60
6.3.1	Motivations	60
6.3.2	General guidelines	61
6.3.3	Key factors and best practices	62
6.3.4	System life cycle	64
6.4	Proposed framework validation	67
6.4.1	Hypothetical case study	67
6.4.2	Real-world project	71
6.5	Opportunities and limitations	73
6.6	Summary	74

6.1 INTRODUCTION

In this chapter, we start by introducing a set of arguments in favoure of the formulated **FbD** efficiency hypothesis (See Chapter 5, Section. 5.6), then, we present an improved Forensic-by-Design frameworks based on our findings. Afterwards, we validate our proposition with both an hypothetical case study and an analysis of a real world project. Finally, we investigate the proposed framework's opportunities and limitations.

6.2 HYPOTHESIS ARGUMENTS

In the previous chapter, we formulated an hypothesis on **FbD** efficiency in some types of systems. Indeed, we hypothesize that: *(a) this new alternative is not effective for some open boundaries systems, and (b) this strategy is not fully aligned with the systems and software engineering standards.*

The aforementioned hypothesis is a conjunction of two claims (a) and (b). Therefore, we will first argue in favour of the claim (a) then (b). The main argument to prove (a) is to find a system or a type of systems that even if designed and developed using the **FbD** paradigm, such a system (or type of systems) will still not be forensic-ready.

Intuitively, we have opted for Cloud Computing Systems (CCS) (Mell and Grance, 2011) which are by default open boundaries systems —*not especially in the perspective of territoriality, but also in the scope of security, control and governance*, and are often scaled across multiple jurisdictions.

Once the type of systems is selected, the next step is to prove that such systems even if designed following the FbD paradigm will still not be forensic-ready. For this purpose, rather than proving directly that such a system can not be forensic-ready, we prove that it possesses at least one or a set of challenges that can not be resolved by any combination of the FbD key factors, and therefore can not be forensic-ready.

So, in the following subsection, we will first select a classification of Cloud Forensics challenges, and then proceed to a mapping between CF challenges and the FbD framework key factors.

6.2.1 Key factors & Challenges Mapping

In this phase, we proceed to a mapping between CF challenges and FbD key arguments that justify our choice. We have, actually, opted for Herman et al., 2020 classification as a source of CF challenges for the following reasons:

1. As stated in Table. 4.2, Herman et al., 2020 study provides the most exhaustive and enumerative classification (9 categories and 65 challenges);
2. Choo, Herman, et al., 2016 have already pointed out some opportunities from combining the FbD framework and a draft of Herman et al., 2020 publication towards the achievement of Cloud Forensics Reference Architecture (CFRA);
3. Herman et al., 2020 is based on the Cloud computing reference architecture (Liu et al., 2011) (see Chapter. 2 Section.2.3) and takes in consideration: (1) a variety of stockholders, (2) multiple characteristics of Cloud computing (e.g., service and deployments models), (3) the involvement of other Cloud actors, such as Cloud Broker and Cloud auditor;
4. Herman et al., 2020 classification; and Ruan and Carthy, 2013a contribution provide together a good basis for a sharpened vision of Cloud Forensics. In fact, while Ruan and Carthy, 2013a work provides a set of DFI scenarios in Cloud computing environments (see Figures. 6.1, 6.2, and 6.3), Herman et al., 2020 states the potential challenges that may emerge from conducting a DFI in such environments.

Table. 6.1 shows a mapping (Herman et al., 2020) Cloud Forensics challenges with (Rahman, Glisson, et al., 2016) Conceptual Forensic-by-Design framework key factors. Note that labels correspond to: Risk management principles and practices (F1), Forensic readiness principles and practices (F2), Incident handling principles and practices (F3), Laws and regulations (F4), Hardware and software requirements (F5), Industry-specific requirements (F6), and Emphasized challenges are considered persistent. Simply put, the persistence of these challenges comes from the fact that none of the possible combinations of FbD key factors can resolve them.

As for potential DFI scenarios in CCS, Figures. 6.1, 6.2, and 6.3 show three cases.

In the first scenario, a CSP offers its services to a cloud consumer (CC) through a cloud carrier (CR), resulting interactions are governed by Service Level Agreements (SLAs) (R_1 and R_2). In the second scenario, multiple CSPs interact with a Cloud Broker (CB) via SLAs (R_i). The relation between the CB and the CC is governed by (R'_1). Scenario 3 describes the interactions among a linear chain of cloud entities. In all these scenarios, a cloud auditor (CA) may be involved to audit the signed SLAs. Investigation may be internal between the provider(s), broker, and the consumer on the shared system, or initiated by law enforcement (LE) towards one of the implied actors. Finally, External Aid (EA) may be invoked to enhance the forensic capabilities in case of investigation.

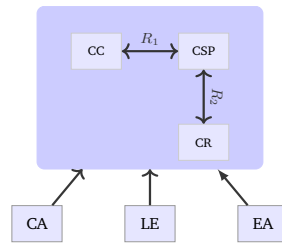


Figure 6.1. Potential DFI scenario 1. Adapted from (Ruan and Carthy, 2013a)

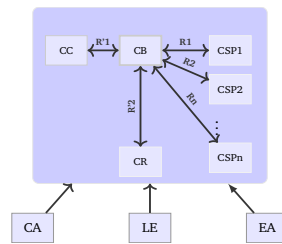


Figure 6.2. Potential DFI scenario 2. Adapted from (Ruan and Carthy, 2013a)

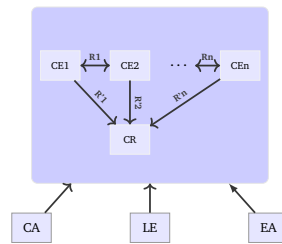


Figure 6.3. Potential DFI scenario 3. Adapted from (Ruan and Carthy, 2013a)

CF challenges	Associated factors	Remarks
Analysis challenges		
Evidence correlation	None	Correlating activities across cloud providers is challenging. Interoperability is also a major issue.
Reconstructing virtual storage	F2, F3, F5, F6.	However, data segregation in a multi-tenants environment is complex. Additionally, data access is problematic. Reconstruction also implies remote or live forensic, which may face jurisdiction challenges.
Timestamps synchronization	None.	However, some of the Cloud computing orbiting technologies such as Cloudlot bring unusual log format, in addition to the already existent proprietary formats. Privacy concerns in case of multi-tenants environment, and data common fields (creation and access date) changes due to migration to and within the cloud.
Log format unification	F2, F5	
Use of metadata	F1, F2, F3, F6.	
Log capture	F2, F3, F5	
Architectural challenges		
Deletion in the cloud	F2, F3	Attributing deleted data to a specific user is challenging.
Recovering overwritten data	F2, F3	Data recovery in a multi-tenant virtual environment is challenging.
Interoperability issues among providers	F5, F6.	Past cloud providers outages demonstrate the need for resiliency. Especially in case of dependency.
Single points of failure	F2, F3, F5	
No single point of failure for criminals	F1	Possibility of a criminal usage of an aggregate cloud providers to commit a cyber-crime.
Detection of the malicious act	F3	Using low cost Cloud resources to launch cyber attack. Authentication mechanisms should link a user virtual identity to a real identity. However, anonymity layer may amplify this challenge.
Criminals access to low cost computing power	None	
Real-time investigation intelligence	None	Events sensing and detection seems problematic in a linear chain of cloud entities.
Malicious code may circumvent VM isolation methods	F1, F3	Laws, regulations and multi-jurisdictions issues
Errors in Cloud management portal configurations	F1, F3	
Multiple venues and geo-locations	F3	
Lack of transparency	F3,F5	
Criminals can hide in cloud	None	Anonymity and data obfuscation.
Cloud confiscation and resource seizure	F1, FF2, F3, F5, F6	
Potential evidence segregation	F4	The maintain of business continuity, and multi-tenancy issues
Boundaries	None	Multi-tenancy issues.
Secure provenance	None	System boundaries need to be define issues. Cloud computing systems are by de facto open boundaries systems.
Data chain of custody	F3, F5, F6	
	None	

CF challenges (Continued)	Associated factors	Remarks
Legal challenges		
Missing terms in contract or SLA	F4	
Limited investigative power	F4	Especially in cross-borders data access
Reliance on cloud providers	F4	In a chain of Cloud service provider, it is impracticable to subpoena multiple (domiciliated, or foreign) Cloud services providers.
Physical data location	F2, F3, F4, F5	Data localisation is challenging. Also, Forensics image acquisition is problematic due to privacy rights of other tenants.
Port protection	F5, F6	
Transfer protocol	F4, F5	
E-discovery	F4, F5	
Lack of international agreements & laws	F4	Cross-borders data access challenge.
International cloud services	F4	
<i>Jurisdiction</i>	F4	
International communication	F5	Complexity and latency in formal mechanisms for cross-borders data access
Confidentiality and PII	F1, F4, F5, F6	
Reputation fate sharing	F1, F4, F2, F3	In a multi-tenants environment, a user may impact the reputation of the host, or other tenants.
Data collection challenges		
Decreased access and data control	F2, F3	Cloud consumers have little or no knowledge of the physical location of their data
Dynamic storage	F2, F3, F6	
<i>Chain of dependencies</i>	None	
Locating evidence	F2, F3	Incident responders face the data localisation challenge.
Data location	F2, F3, F4, F5	Cloud providers store multi-tenants data in virtualized environment across multiple data centers in multiple jurisdictions.
Imaging and isolating data	F2, F3, F5, F6	Lack of a mature and established solution for Cloud forensics image acquisition in some Cloud service models other than IaaS.
Data available for a limited time	F5	
Locating storage media	F2, F3, F5	
Evidence identification	F2, F3, F5	
Live forensics	F5	Data location, multi-tenancy and jurisdiction challenges.
Resources abstraction	F1, F2, F3	Digital evidences sources are in fact dependent on the associated service model (IaaS, PaaS, or SaaS) and on the deployment model too.
Application details are unavailable	F5, F6	Transparency.
Additional evidence collection	F2	
Imaging the cloud	F2, F3, F4, F5	Impracticable in SaaS and PaaS service models.

CF challenges (Continued)	Associated factors	Remarks
Data collection challenges (Continued)		
Selective data acquisition	F2, F3, F5, F6.	Multi-tenancy challenge.
Cryptographic key management	F2, F3, F5.	Data obfuscation.
<i>Ambiguous trust boundaries</i>	None	Trust issues.
Data integrity and evidence preservation	F2, F3, F5.	Chain of custody
Root of trust	F2, F3, F4	Trust issues
Role management challenges		
Identifying account owner	F1, F2, F3, F5	Transparency and trust issues.
<i>Fictitious identities</i>	None	Data obfuscation and anonymity layers.
Decoupling user credentials & physical location	F2, F3, F5	Transparency and trust issues.
Authentication and access control	F2, F3, F5	Need for security control.
Standards challenges		
<i>Testability, validation, and scientific principles not addressed</i>	None	Related to investigation tools, model and practices
<i>Lack of standard processes and models</i>	None	No established Cloud DFI model.
Training challenges		
Cloud training for investigators	F2	However, valid cloud investigation solutions are not yet present.
<i>Limited knowledge of logs and records</i>	None	Training challenges.

Table 6.1. Mapping (Herman et al., 2020) CF challenges with (Rahman, Glisson, et al., 2016) framework key factors.

In the following subsections, we first provide a precise description of what is a *persistent challenge*, and then analyse the result of the aforementioned mapping (see Table.6.1).

6.2.2 Persistent Challenges Filtering

In this step, Herman et al., 2020 challenges were analysed sequentially in the scope of potential DFI scenarios. Each CF challenge is considered for resolution by any potential combination of FbD framework key factors (Rahman, Glisson, et al., 2016). Whenever a CF challenge fails to: **(1) be resolved by any FbD key factors combination, or (2) the proposed combination cannot fully resolve the challenge, the CF challenge is then considered *persistent*.**

Table. 6.1 shows several persistent challenges (emphasized ones). For example, “*Criminals access to low cost computing power*”, and “*Criminals can hide in the cloud*” (Category: Architecture), are challenges that cannot be resolved by any combination of key factors, and cannot even be considered at the earliest stage of a Cloud system life cycle (design) because such challenges emerge at the *Utilization* stage. Other persistent challenges, such as “*Jurisdiction*” and “*Limited Investigative Power*” are partially resolved by the “*laws and regulation*” FbD key factors (F4 see Table. 6.1). However, the literature review shows that: (1) multi-jurisdiction is a complex and persistent CF challenge, and (2) cross-borders data access is complex and mechanisms such as MLAT are sometimes obsolete.

Even if a CF challenge is partially resolved by a combination of FbD key factors in a DFI scenario *A* (see Figures. 6.1, 6.2 and 6.3), it may not be in another scenario *B*, and therefore it is considered persistent.

Hereafter, we proceed to an analysis of the CF challenges and FbD key factors mapping.

6.2.2.1 Mapping Results Analysis

The *Missing terms in contract or SLA* is one of those persistent CF challenges that may impact the success of a DFI. In fact, even in the simple case (see Figure. 6.1), if we consider a Cloud system that integrates the services of a Public Cloud Service Provider (CSP), then access to digital evidence depends on the trustworthiness of the CSP. Moreover, issues such as multi-tenancy and multi-jurisdictions may undermine the success of a DFI. For a Cloud system relying on a third party (or system elements) that makes sensitive data (or potential digital evidence) out of its control border, such a system cannot be forensic-ready even if designed with the due FbD specification.

Some CF challenges (Table 6.1), such as boundaries, missing terms in contract or SLA, training, etc. confirm the Forensic-by-design framework insufficiencies (Alenezi et al., 2017). Additionally, challenges, such as confidentiality and PII, data integrity, and evidence preservation, single point of failure, etc. indicate the requirement for security, privacy, and resiliency.

Table. 6.1 suggests also the dominance of the architectural concerns. Moreover, we note that transparency and boundaries are considered among the most complex issues. In fact, boundaries in Cloud computing systems need to be redefined (Herman et al., 2020) ; whether to separate

users' data in a multi-tenants environment, specify data storage in multiple jurisdictions, or to define a security perimeter for boundary control (M. L. Badger et al., 2012). Actually, boundary definition is problematic in some cases. For instance, it is easier in the case of a simple customer-provider relation (see Figure. 6.1) than in the case of a transitive relation between a customer and multiple providers (see Figure. 6.2).

Cloud systems that integrate (or rely) on Public (or community or hybrid) Cloud Services (or resources) Provider(s) cannot ensure the continuous monitoring of a potential Forensic-ready state because some of its functionalities are out of its governance and control boundaries scope.

Therefore there is, at least, a category of open boundaries system for which the FbD framework may not be efficient. This observation does therefore confirm the first part of our hypothesis.

6.2.2.2 Candidate key factors

In this step, we propose adding three candidate key factors (security, privacy, and resiliency) in order to: (1) address some of the persistent CF challenges, and (2) remedy to some of the FbD insufficiencies (Alenezi et al., 2017; Grispos, Garcia-Galan, et al., 2017; Pasquale et al., 2018) (see Table. 5.3). Note that the first two key factors that we propose (security and privacy) already appear in Grispos, Glisson, and Choo, 2017. Our choice is moreover justified by the following reasons.

First, the *security* key factor was considered for the following reasons:

1. DFR is assumed on proper security measures (see Rowlingson 2004, (p. 9));
2. There are similarities between Security-by-design and Forensic-by-design (Rahman, Glisson, et al., 2016), and therefore potential opportunities from their conjunction;
3. Most importantly, many CF persistent challenges would be resolved with some appropriate security measures.

As for the *Privacy* key factor, our choice was motivated by the following observations:

1. Many CF persistent challenges would be resolved with the appropriate privacy safeguard techniques;
2. Like Security-by-design, Privacy-by-design presents some similarities with Forensic-by-design, and therefore opportunities may emerge from their conjunction as well.

Finally, we propose the addition of "*Resiliency*" as a third key factor. This choice is motivated by the existence of challenges such as *Single point of failure*, *No single point of failure for criminals*, and *Chain of dependency* (see Table. 6.1), and the existence of scenarios where there is either a single point of failure such as a Cloud broker (see Scenario. 6.2) or a chain of dependencies (see Scenario. 6.3).

Note that we do not consider the "*safety*", and "*medical*" key factors cited in Grispos, Glisson, and Choo, 2017 as they are either industry-related or application domain specific key factors.

Moreover, it is not practical to examine each persistent challenge and add some key factors that may resolve it. Such an approach will for sure lead to a huge number of key factors, and therefore the emergence of new challenges related to either requirements elicitation or performance overhead. In other words, we believe that it would be better to have a minimal set of key factors to resolve these persistent challenges, than to consider every imaginable key factor for it will constitute real hurdles to be surmounted during the system's development and its monitoring.

Details on the added key factors (Security, Privacy and Resiliency) and their associated standards and best practices are provided in Subsection. 6.3.3. In the next subsection, we discuss the alignment of FbD with the systems and software engineering standards.

6.2.3 FbD alignment with SE standards

In their proposition, Rahman, Glisson, et al., 2016 proposition, the authors formulated *What* is required for the integration of the forensic requirements during the design and the development of a system. However, questions on the *How, When and Where* are still unanswered. In fact, the authors did not explicitly state a standard to follow, or to comply with during the system's life cycle. On the other hand, there are two standards (*Systems and software engineering — Software life cycle processes 2017*; *Systems and software engineering — System life cycle processes 2015*) on systems and software engineering. While the first addresses systems life cycle processes, the second is more dedicated to the software. The aforementioned standards define 6 stages for a system (or software) life cycle: (1) Concept, (2) Development, (3) Production, (4) Utilization, (5) Support, and (6) Retirement. In addition to four groups of processes that may be enacted during any stage. These include: Agreement processes; Organizational Project-Enabling Processes; Technical Management Processes; and Technical Processes.

As stated in the formulated hypothesis, we believe that FbD is not fully aligned with System Engineering (SE) standards at least for the following reasons:

- 1) **Structure, iteration, and recursion::** A system is composed of multiple elements referred to by "*System elements*" and during a system's life cycle, there may be a need for an external resource or service and hence establishing connections with other systems that are referred to by "*Enabling systems*". Therefore, achieving a *forensic-ready* system cannot be feasible while ignoring the system's structure. Additionally, taking into consideration the structural aspect of the system to be built implies the application of some processes and tasks in an iterative and recursive fashion. Details on the impact of these aspects are provided in subsubsection. 6.2.3.1;
- 2) **Stages, processes, and activities::** Design and development are two stages (among others) in the system of interest's life cycle. Moreover, there are recursive pathways between a system's life cycle stages. Actually, there might be a need to return to the design and development stages in some cases such as: (1) the evolution of users and stakeholders needs, (2) the emergence of new threats, or (3) technological advancements. Therefore,

restricting the continuous monitoring of the system's *forensic-ready* state to the first stages may be problematic. Details on these aspects are provided in subsubsection. 6.2.3.2;

- 3) **Validation and Verification::** These two processes are important in the system of interest's life cycle. In fact, together they guarantee that the right system is built and that it is built right. However, as we may see hereafter in Sub-subsection 6.2.3.3, the application of these processes has been restrained in the previous framework (Rahman, Glisson, et al., 2016). Details on validation and verification aspects are provided in subsubsection. 6.2.3.3.

The above three arguments are detailed below.

6.2.3.1 Structure, iteration, and recursion

The FbD framework (Rahman, Glisson, et al., 2016) may be modelled as a set of key factors or requirements that are integrated during the design and development stages of a system, with a constant and continuous monitoring of the desired *forensic-ready* state via controls (verification and validation). However, this framework does not take into consideration an essential system's characteristic which is *Structure*. In fact, in SE the desired system to be built (System of Interest) is considered as a set of interacting *Systems elements* and *Enabling systems* (see Figure. 6.4). Therefore, this FbD framework is either considering a system as an indivisible single bloc, or misses the required composition or *integration* constraints of the system's structure. In other words, if FbD is applied iteratively and recursively to each system element, does this necessarily guarantee that the composed system of interest will be forensic ready?

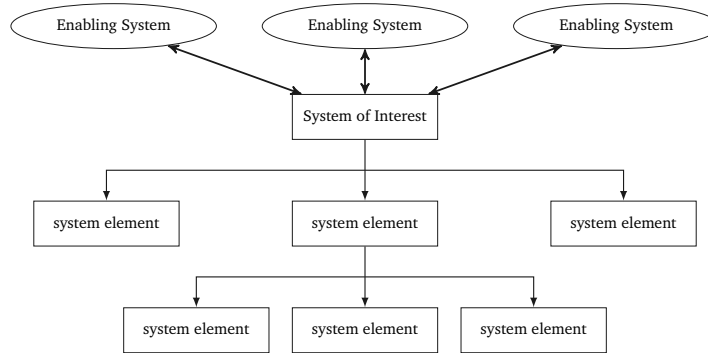


Figure 6.4. A system of interest structure.

Additionally, the missed system's *structure* as an essential characteristic leads to some of the FbD insufficiencies. For example, the architectural challenges (see Alenezi et al., 2017 and Table. 6.1) are linked to the system's structure, as do some of the data collection challenges.

Considering the system of interest as a set of interacting elements (system elements and enabling systems) implies the application of some "*treatments*" (processes) iteratively and recursively till reaching an atomic element. For instance, requirements engineering processes

are applied in an iterative and recursive manner (see *Systems and software engineering — Life cycle processes – Requirements engineering 2018*, (sec. 5.3.1)).

Finally, ignoring some parts of the system of interest (enabling systems) may obfuscate important processes related to the acquisition and supply and eventually their associated contracts and agreements. The missed SLA aspect in the FbD framework is rightfully stated in both Alenezi et al., 2017 work and in Table 6.1.

6.2.3.2 Stages, processes, and activities

From the perspective of Systems engineering standards, a system's life cycle contains multiple stages (conception, development, production, utilization, etc.). However, the FbD framework by Rahman, Glisson, et al., 2016 focuses only on the earliest stages (design and development). Focusing on only two stages is equivalent to making abstraction of the other stages and eventually of the recursive pathways between stages. In fact, it is not strange to return to the design and the development stages even in the utilization one whenever there is an evolution in the stakeholders (or users) needs, an emergence of new threats, or a need to integrate new advanced technologies, etc. Therefore, the continuous monitoring of the desired *forensic-ready* state should be required throughout the system of interest's life cycle, rather than restricted to the exit from its first two stages.

If the integration of forensic requirement is done through the entire system's life cycle, then issues such as "*Assessing the influence of Forensic-by-Design on the Forensic Readiness Ecosystem*" (see Grispos, Garcia-Galan, et al., 2017) will not be considered because DFR efforts in the production (or utilization) stage will be the continuation of the initiated efforts at the design and development stages.

Additionally, there is no indication of the impact of the FbD key factors on some processes, such as requirements analysis, architecture definition, design definition, etc. In fact, FbD is centred on the design and development stages without specifying a development strategy (Once-through, Incremental, Evolutionary) or methodology (e.g., waterfall, spiral, etc.).

6.2.3.3 Validation and Verification

In Rahman, Glisson, et al., 2016 FbD framework, the verification and validation processes are related to: (1) the reliability and adequacy of the collected evidence, (2) the soundness of the used functions for the collection. Therefore, the verification and validation processes are given another usage rather than the one specified in the SE standards.

Even if we consider that the FbD defined verification and validation processes as sub-processes of SE verification and validation processes, there is still the issue of jurisdiction. In fact, while the FbD framework attaches the reliability of the collected evidence and the soundness of the used functions to the verification and validation processes, it omits (or makes abstraction of) the associated jurisdiction laws and regulations. Moreover, the multi-jurisdictions aspect is a complex and persistent challenge in the case of Cloud computing systems. These

observations led us to propose a new Forensic-by-design framework that we describe in detail in the next Section.

6.3 THE PROPOSED FRAMEWORK

In this section, we propose a Forensic-by-design framework for Cloud computing systems (Figure. 6.5). The *System of interest* is a reference to a Cloud system or any system that is built using the proposed framework. Therefore, we will address the following points:

1. Motivation.
2. General guidelines.
3. Key Factors and best practices.
4. System's life cycle and System development life cycle (SLDC).
5. Validation.

6.3.1 Motivations

Upon the formulation of the initial hypothesis on FbD effectiveness for some class of open boundaries systems, we confirmed our intuition by proving that: (1) In the case of Cloud computing systems, there are multiple CF challenges that cannot be resolved by any combination of FbD key factors (see Subsubsection. 6.2.2.1), and (2) FbD as presented by Rahman, Glisson, et al., 2016 is not fully aligned with SE standards (see Subsection. 6.2.3).

Therefore, our main motivation was to propose a new Forensic-by-design framework —with some emphasis on Cloud computing systems— that does not only focus on integrating the forensic requirements into the system's life cycle stages (*What*), but also enforces compliance with the SE standards (*How*).

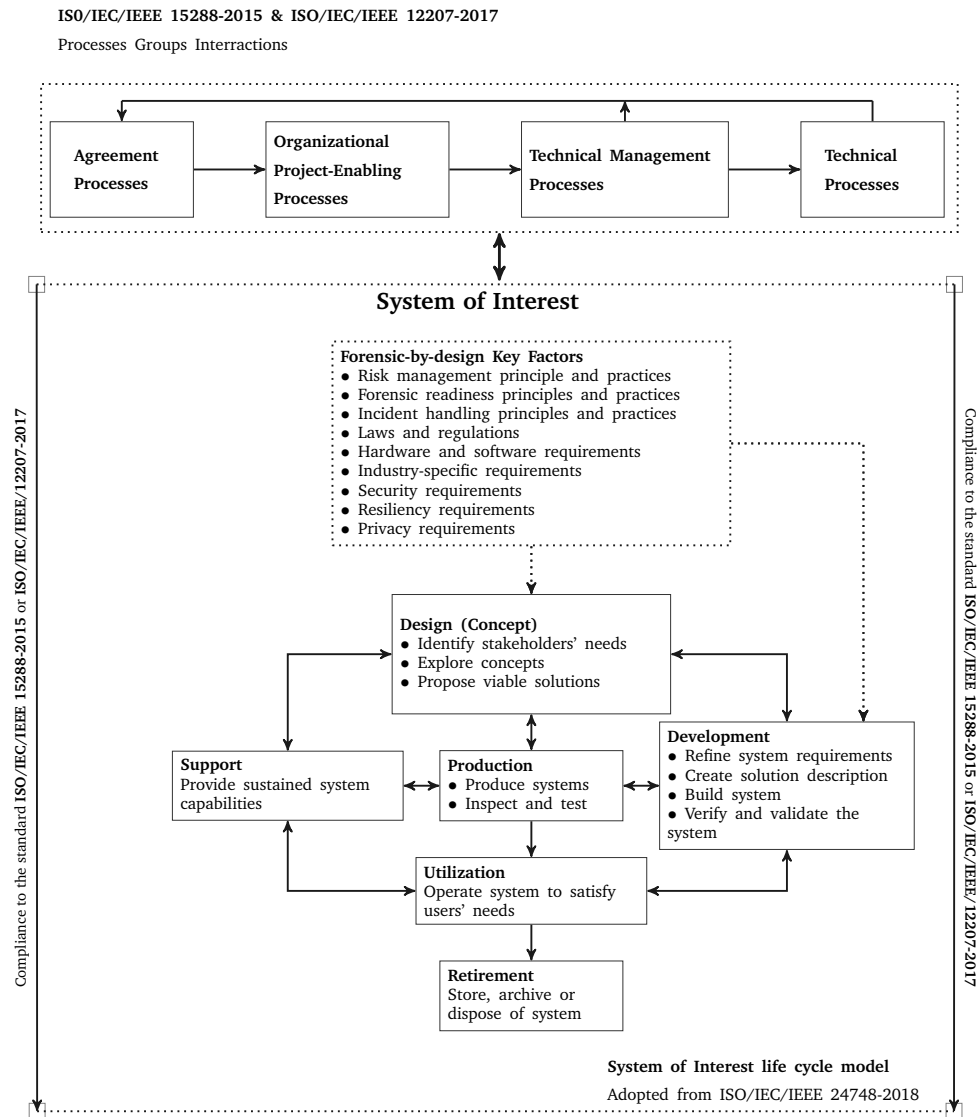


Figure 6.5. A Forensic-by-design framework for Cloud computing systems.

6.3.2 General guidelines

As stated in the proposed framework (see Figure. 6.5), after selecting the system of interest's life cycle model in compliance with the *Systems and software engineering — Life cycle management — Part1: Guidelines for life cycle management 2018* standard, the conception and development of the system is made in accordance to either *Systems and software engineering — System life cycle processes 2015*, or *Systems and software engineering — Software life cycle processes 2017* and the

compliance to these standards should be ensured along the system's life cycle. For this purpose, we recommend the following guidances:

1. Compliance to the *Systems and software engineering — Life cycle management — Part1: Guidelines for life cycle management 2018* standard;
2. Compliance to either *Systems and software engineering — System life cycle processes 2015*, or *Systems and software engineering — Software life cycle processes 2017*, and enactment of the associated groups of processes whenever required;
3. Ensure that the associated key factors best practices and standard are preferably aligned with the above SE standards and cover all the system of interest life's cycle stages;
4. Select the appropriate development strategy (Once-through, Incremental, Evolutionary) in addition to the system's development life cycle methodology;
5. Ensure a continuous monitoring of the desired system of interest's forensic-ready state via: (1) validation and verification processes; and (2) recursive pathways in the selected system's life cycle model.

In what follows, we provide details on the adopted key factors and their associated standards and best practices.

6.3.3 Key factors and best practices

As shown in Figure. 6.5, the proposed framework contains 9 key factors. The first 6 ones are the ones already proposed by Rahman, Glisson, et al., 2016, the new 3 ones are the ones that we have proposed earlier (Security, Privacy, Resiliency). However, Grispos, Glisson, and Choo, 2017; Rahman, Glisson, et al., 2016 do not provide many details on the associated standards and best practices of their proposed key factors (See Table 5.2). More importantly, these works do not explicitly state to which extent the adopted practices are in compliance with the system and software engineering standards

Considering the three added key factors, first, we should state that the privacy one was first brought by Grispos, Glisson, and Choo, 2017 for a Forensic-by-design Medical Cyber Physical Systems (MCPS). However, we argue here the for addition of this key factor for the following reasons: (1) there is a need for privacy requirements integration during a system's life cycle (e.g., protect Personal Identifiable Information (PII) and biological indicators gathered by sensors that are subject to privacy laws and regulations), (2) the opportunities that may emerge from similar existing paradigms, such as "Privacy-by-design" (Cavoukian, 2012) and "Privacy engineering" (Shapiro et al., 2014). For the integration of this key factor, we recommend using frameworks such as the NIST, 2020 and the *Information technology — Security techniques — Privacy engineering for system life cycle processes 2019* standard.

As for resiliency, it was hinted as part of the risks management requirements (Rahman, Glisson, et al., 2016). However, we believe that it deserves to be a key factor on its own (see

Subsubsection. 6.2.2.2). Indeed, resiliency measures are required to ensure the continuity of the business operations, the safeguard of digital evidence, and the maintenance of a good standing to the signed SLAs. Therefore, propositions that align cyber-resiliency to a system's life cycle standard such as those provided by Ross, Pillitteri, et al., 2019 may be appropriate for this purpose.

Finally, the necessity to integrate *security requirements* into a system's life cycle has led in the past to the emergence of the *Security-by-design* paradigm. Encouraged by the conceptual similarities between Forensic-by-design and *Security-by-design* (see Subsubsection.6.2.2.2), we recommend the adoption of propositions (e.g., Ross, McEvelley, and Oren, 2018) that align security requirements with a system's life cycle. To summarize, Table. 6.2 provides some of the standards and best practices associated with the above mentioned key factors. Note, however, that it is not realistic to list all the laws and regulations that are related to Cloud systems among multiple jurisdictions, as it is also impractical to cite all the standards and best practices related to "*Hardware and software*" and "*industry specific*" key factors.

Key Factor	Standards and best practices
Risk management	Initiative 2018; <i>Systems and software engineering — Life cycle processes — Risk management</i> 2006; NIST 2018
Forensic readiness	<i>Information technology — Security techniques — Incident investigation principles and processes</i> 2015; Rowlingson 2004; Valjarevic and Hein Venter 2013, etc.
Incident handling	<i>Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management</i> 2016; <i>Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response</i> 2016; <i>Information technology — Security techniques — Incident investigation principles and processes</i> 2015
Laws and regulations	General Data Protection Regulation (GDPR) (Regulation, 2016), Health Insurance Privacy and Accountability Act (HIPAA) (Act, 1996), Clarifying Lawful Overseas Use of Data (CLOUD) Act (U.S.A DOJ, 2018), etc.
Hardware and software requirements	-
Industry specific requirements	-
Resiliency requirements	Ross, Pillitteri, et al. 2019
Security requirements	Ross, McEvelley, and Oren 2018
Privacy requirements	Cavoukian 2012; <i>Information technology — Security techniques — Privacy framework</i> 2011; <i>Information technology — Security techniques — Privacy engineering for system life cycle processes</i> 2019; NIST 2020; Shapiro et al. 2014

Table 6.2. FbD Key factors associated standards and best practices.

The next section provides details on a system of interest's life cycle and recommendations on its SDLC.

6.3.4 System life cycle

The *Systems and software engineering — Life cycle management — Part1: Guidelines for life cycle management* 2018 standard provides a description of the system (or software) life cycle stages, enumerates the activities and tasks of each stage, and points out the processes that may be enacted. For example, the purpose of the concept (design) stage is to provide the preliminary system requirements, and a feasible architecture, and a design solution. In some cases, parts of the designed solution may be eventually acquired from external providers. So, among the processes that may be enacted during this stage, there are at least *the agreement processes group*,

stakeholder needs and requirements definition process, *architecture definition* process, etc. However, at this point, the integration of the stated key factors is not done yet. For this purpose, it is required that the associated key factors best practices to be aligned to the systems and software engineering standards.

Table 6.3 gives an example on how to integrate the proposed framework's key factors during a task which is specified by the following: (1) **Stage**: design; (2) **Process**: Architecture definition ; (3) **Activity**: Assess architecture candidate ; (4) **Task**: Assess each candidate architecture against constraints and requirements. (See *Systems and software engineering — Software life cycle processes 2017*; *Systems and software engineering — System life cycle processes 2015* Section 6.4.4.3 e).

Task : Assess each candidate architecture against constraints and requirements.
Security : Assess each candidate architecture against the security requirements and security-related constraints (Ross, McEvilley, and Oren 2018, Section AR-5, pg 123).
Resiliency : Ross, Pillitteri, et al. 2019 see F.2.4, pg 149
Privacy : <i>Information technology — Security techniques — Privacy engineering for system life cycle processes 2019</i> , Section. 6.8; Identify architectural, technical point, and policy privacy controls (Shapiro et al., 2014).
DFR : Defining system architecture (<i>Information technology — Security techniques — Incident investigation principles and processes 2015</i> , Section 7.7)

Table 6.3. The proposed framework's key factors integration.

Nonetheless, during the design stage, and upon stakeholders needs inventory and diverse constraints enumeration; the system architect proceeds to the definition of the system requirements. Afterwards, the system development is initiated, and is guided by the nine adopted key factors. During the development stage, the validation process is enacted to confirm that the built system meets the stakeholders' needs (the right system is built), and the verification process is enacted to confirm that the system is built right (*Systems and software engineering — Software life cycle processes 2017*; *Systems and software engineering — System life cycle processes 2015*). These two processes also assess the desired *Forensic-ready* state, and serve as an exit criteria towards the following stages.

Depending on the selected development strategy and SDLC model, there are multiple phases to undergo before reaching the utilization stage. In this section, we will focus on the three following common phases: (1) Requirements Engineering, (2) Architecture Definition, and (3) Design definition.

6.3.4.1 Requirements engineering

Requirements engineering is an interdisciplinary function that covers activities related to requirements (e.g., discovery, elicitation, analysis, verification, etc.), and thus along the system

of interest's life cycle. This function is carried out in an iterative and recursive way—in accordance with the system structure. The *Systems and software engineering — Life cycle processes – Requirements engineering 2018* standard addresses the requirement engineering activities along the system's life cycle and is aligned with *Systems and software engineering — System life cycle processes 2015*, and *Systems and software engineering — Software life cycle processes 2017* standards. Additionally, these two standards provide two processes: (1) *Stakeholder needs and requirements definition* process, and (2) *System requirements definition* process.

Among the “*Stakeholder needs and requirements definition*” process application outcomes we may cite: stakeholder identification, identification of constraints on system, Stakeholder needs identification, etc. As for the application of the *System requirements definition* process some of the expected outcomes are: system requirements (functional, performance, process, non-functional, and interface), system description (interface, boundaries, solution), enabling systems, etc.

Multiple stakeholders may express concerns about the system of interest. Needs are transformed into requirements, constraints on the system and other constraints (technological, agreement, integration) are included. Once the requirements are analysed, then a candidate solution is designed. Some issues related to the forensic requirements elicitation and analysis were expressed by Grispos, Garcia-Galan, et al., 2017 (see Table. 5.3), these issues may be resolved using elicitation techniques such as those described in *Systems and software engineering — Life cycle processes – Requirements engineering 2018*, sec 6.3.3.5 standard, by adopting a scenario based technique as stated in Rowlingson, 2004, or a process inspired from Omeleze and Hein S. Venter, 2017 and Kebande, Baror, et al., 2020. Additionally, for non-functional requirements like security, frameworks such as those proposed by Haley et al., 2008; Ross, McEvelley, and Oren, 2018 may be adopted. Finally, there are also formal methods for requirement engineering to be considered.

6.3.4.2 Architecture definition

The purpose of this process is to generate system architectures alternatives, assess, and select the architecture that frames stakeholders needs and satisfies system requirements. Among the expected outcomes from this process, we may cite: (1) architecture viewpoints and views, (2) system elements and their interfaces, and (3) context, boundaries, and external interfaces. During this process, the integration of some of the proposed key factors is required. In fact, Ross, McEvelley, and Oren, 2018; Ross, Pillitteri, et al., 2019 already address the integration of security and resiliency key factors into a system's life cycle and provided guidelines for incorporating these two key factors even in the architecture definition process. An example on how the proposed key factors are integrated into the system of interest's life cycle is shown in Table. 6.3.

In conjunction with this process, the *Systems and software engineering — Architecture description 2015* standard provides guidelines on the architecture description that we recommend during this phase.

6.3.4.3 Verification and Validation

Verification and *Validation* are two important processes that belong to the technical processes group. While the verification process aims to determine that “*The product is built right*”, the validation process aims to determine that “*The right product is built*”. The application of these two processes is done in a recursive and iterative manner on the system of interest’s structure along its life cycle, and may be used as an exit point from one stage to another.

The verification process identifies anomalies (errors, defects, faults) in any information item, system elements, life cycle processes, etc. Some of its expected outcomes, as stated in *Systems and software engineering — System life cycle processes 2015*, are: anomalies identification, enabling systems verification, system elements verification, etc. Note that, in Rahman, Glisson, et al., 2016, this process is given a restricted scope. Therefore, we argue that this process may include all kinds of verifications (security, privacy, forensic, resiliency). In fact, Ross, McEvelley, and Oren, 2018; Ross, Pillitteri, et al., 2019 already proposed the integration of the security and resiliency verifications. Additionally, we note that DFR verification is present in *Information technology — Security techniques — Incident investigation principles and processes 2015*, sec.7.12.

The validation process aims to provide objective evidence that the system, when in use, will fulfil its business objectives and stakeholders requirements. Among its main expected outcomes (*Systems and software engineering — System life cycle processes 2015*) we may cite: definition of validation criteria, system elements validation, availability and validation of any enabling system or service, etc. The scope of this process was also restrained in Rahman, Glisson, et al., 2016. Similarly to the verification process, we suggest the inclusion of all kinds of validations (security, privacy, forensic, and resiliency). For this purpose, we recommend compliance to guidelines, such as Ross, McEvelley, and Oren, 2018, Ross, Pillitteri, et al., 2019, and *Information technology — Security techniques — Incident investigation principles and processes 2015* standard.

The next Subsection provides a validation of the proposed framework.

6.4 PROPOSED FRAMEWORK VALIDATION

To validate the proposed framework, we first state an hypothetical case study (Intelligent Transportation System), and provide recommendations on how to integrate the proposed key factor during an ITS life cycle. Afterwards, we analyse a real-world ITS project and discuss the common points and similarities with the proposed framework.

6.4.1 Hypothetical case study

Let us extend the hypothetical scenario provided by Rahman, Glisson, et al., 2016 to an Intelligent Transportation System (ITS) (Figueiredo et al., 2001). A vehicular network (or vehicular cloud) (Olariu, Hristov, and Yan, 2013) is a component of an ITS among other parts, such as the intelligent signalization, transportation management, traveller management, etc.

The implementation of an ITS induces certainly a large deployment of sensors and actuators. Therefore, huge data volumes flow with a requirement for real-time data analysis and decision making support. ITS issues are multiple. For instance, security, privacy, and resiliency are among the top ITS persistent challenges (Ganin et al., 2019; Petit and Shladover, 2014).

In a typical ITS, data is aggregated from multiple heterogeneous sources (On Board Unit (OBU), Road Sensors Units (RSU), Vanets infrastructure, control centres, roads cameras, etc.). Because of the consequent data volumes, the ITS system architect may opt for Cloud solutions. We suggest the use of a Cloud broker architecture (see Figure. 6.2). Tables. 6.4 and 6.5 summarize some actions to perform when applying the proposed framework for the design of an ITS system. Focus will be essentially on the vehicular network (vehicular cloud) and on the supporting Cloud computing system (cloud broker). Still, the proposed framework may be applied iteratively to other components of the ITS.

Note, however, that the *Integration process* (*Systems and software engineering — Software life cycle processes 2017*; *Systems and software engineering — System life cycle processes 2015*) must still be enacted in a way to preserve the forensic readiness of the assembled system (ITS, in this case).

Design factors	Possible actions
Vanets and Vehicular Cloud	
Risk management principles and best practices	In addition to (Rahman, Glisson, et al., 2016) recommendations, we propose the identification, assessment, and evaluation of security and privacy risks associated with road infrastructure, radars, sensors and signalization, traffic light, etc. We recommend also, the evaluation of any cause that may lead to accidents and traffic disruption (Ganin et al., 2019; Petit and Shladover, 2014).
Forensic readiness principles and best practices	Planning for the identification, collection, examination and analysis of heterogeneous artefacts from multiples heterogeneous sources. In fact, digital evidences sources may be found in the vehicle, roads, signalizations, infrastructure, and command centres. Additionally, there is a need for the development of digital forensic methods and tools tailored for these new <i>devices</i> .
Incident-handling principles and best practices	See. (Rahman, Glisson, et al., 2016)
Laws and regulations	In addition to (Rahman, Glisson, et al., 2016) proposed actions, we suggest a clear and concise digital evidence collection procedure and a periodic evaluation of the staff training, and the assertion of the collected digital evidence with a forensic expert testimony.
Hardware and software requirements	Interoperability is required in order to design digital evidence collection capabilities that suite the multitude of potential evidences sources. Additionally, portability is also of importance. Allowing designed solutions to be applicable for a large range of technologies will reduce its associated learning curve and ease the staff training.
Industry specific requirements	See. (Rahman, Glisson, et al., 2016)
Security requirements	Integrating security principles and practices in the design of devices (OBU, RSU, IOT, Sensors, etc.), communication protocols, infrastructure, etc., will ease some of the ITS security issues.
Resiliency requirements	Assessment and evaluation of resiliency in networks, routing communication, OBU, CDN, and sensors will help to ensure a prompt recovery. Additionally, simulating disaster and failure scenario on the ITS components will help to assess the staff training, evaluate the response delays, and measure the ability to recover.
Privacy requirements	Designing OBU, RSU, sensors, devices, communications protocol, applications, and any ITS subsystems to preserve the conductor privacy, behaviour, and the travellers routines is a necessity.

Table 6.4. Designing an ITS (Vanets recommendations).

Design factors	Possible actions
Cloud broker and CSPs	
Risk management principles and best practices	Identification, assessment and evaluation of security and privacy risks of CSPs (suppliers) and Cloud broker. The compliance of both CSPs and Cloud broker to specific risk management frameworks, such as the Initiative, 2018 is preferred, and may be stated in signed contracts.
Forensic readiness principles and best practices	Under pre-established assumptions, the Cloud broker may be in charge of planning for the identification, collection, examination and analysis of heterogeneous artefacts from multiples CSPs. So, a clear specification of stakeholders may improve the segregation of duties (<i>Who is in charge of What</i>), and provides a concise definition of ownership. Moreover, remote forensic acquisition, and live forensic may be required during the course of a DFI.
Incident-handling principles and best practices	The compliance of CSPs and Cloud broker to the incident-handling best practices (Cichonski et al., 2012) is vital. Moreover, the staff training and CERT teams expertise periodic assessment, either by a Cloud broker or an external auditor, will surely enhance the due reactivity in case of abnormal events.
Laws and regulations	In this case of study, jurisdiction is important. In fact, avoiding the multi-jurisdictions challenge is crucial. Moreover, due to the critical nature of the ITS, federal or governmental considerations arises; compliance to related best practices, such as those proposed by L. Badger et al., 2014 is recommended.
Hardware and software requirements	The Cloud broker must ensure the interoperability and portability of services, while the CSPs must guarantee the traceability and log features of their offered services and software, in addition to the adoption of the Trusted Platform Modules (TPM) for the hardware.
Industry specific requirements	This set of requirements contains at least industrial considerations for CSPs data centers and infrastructure maintenance, standards and best practices for services and software development, policies and regulations for data storage and archives.
Security requirements	To align security considerations with a system life cycle, CSPs may consider Ross, McEvelley, and Oren, 2018 recommendations. However, in the production stage CSPs may also adhere to a minimal security baseline such as those described in Alliance, 2019. Furthermore, the assessment and audit of both CSPs and the Cloud broker security commitments may be envisioned in a bilateral form, or with the help of a Cloud auditor.
Resiliency requirements	Resiliency techniques in Cloud computing infrastructures and applications have already been investigated by studies such as those cited by Colman-Meixner et al., 2016. Thus, the assessment of both CSPs and the Cloud broker compliance to resiliency best practices is vital. Moreover, CSPs may also consider integrating resiliency techniques and measures in relevant life cycle stages and processes (Ross, Pillitteri, et al., 2019).
Privacy requirements	Preserving conductor, travellers, and staff privacy implies using privacy safeguard measures along the data pathways and at each layer of a CSP from the physical to the application level. Therefore, CSPs and Cloud brokers compliance to privacy best practices, standards, regulations and laws, such as those stated in Regulation, 2016 is required and preferably assessed and audited periodically.

Table 6.5. Designing an ITS (Cloud Broker recommendations).

6.4.2 Real-world project

In the following, we provide a similarity analysis between a concrete ITS project example (more precisely Cooperative ITS) and the proposed framework. The Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) (DoT, 2021e) (see Figure. 6.6) was developed by the U.S department of transportation in 1996 and is still updated nowadays.

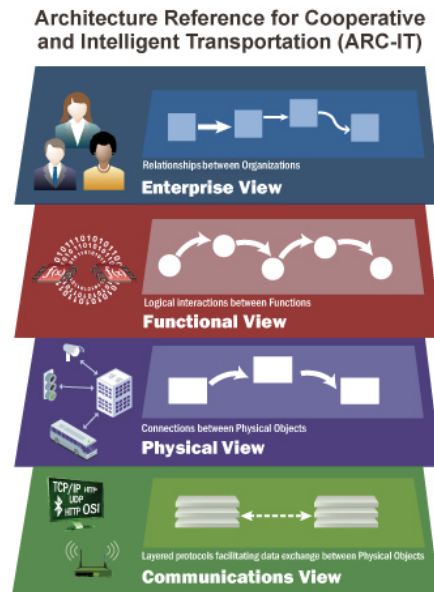


Figure 6.6. ARC-IT architecture (DoT, 2021e).

The ARC-IT is based on the *Systems and software engineering — Architecture description 2015* architecture description standard, and frames multiple stakeholders' concerns and interests. It also contains 4 different viewpoints (Communication, Physical, Functional, and Enterprise), and their associated views. Moreover, it allows different scales of implementation, going from local level to a regional one. Furthermore, the associated ARC-IT document (Team, 2007a) advocates the use of system engineering and the "V" model.

Proposed Framework Propriety	Observations from the ARC-IT project
General guidelines	
System life cycle model	Consider a six stage cyclical system life cycle model inspired by (<i>Systems and software engineering — Life cycle management — Part1: Guidelines for life cycle management</i> 2018) and contains: Project Development (including design), Project Construction (installation), Operations, (Regional) Planning, Maintenance, Retirement/Replacement (see DoT, 2021a).
System Engineering Standards	The <i>Systems and software engineering — System life cycle processes</i> 2015 standard is among the ARC-IT considered SE standards and best practices (see Team, 2007a).
System development life cycle	The V model is the adopted SDLC model, however the development strategy depends on the region and the type of project (see Team, 2007a)
Continuous monitoring	The adopted system life cycle is cyclical, therefore there is a recursive pathway between stages. Additionally, the adopted SE standard contains the Verification & Validation processes. So the continuous monitoring is granted. However, concerning the forensic-ready state, it may be granted if and only if the forensic requirements are integrated into the system life cycle stages.
Validation & verification	Being part of the adopted system engineering processes (see (Team, 2007a)), those processes are enacted. However, due to the fact that DFR requirements are partially integrated in the ARC-IT, there is no details on forensic requirements verification and validation.
Key factors Integration	
Risk management	Integrated during the system life cycle (see Team, 2007a), and considered also in the organizational security controls (see DoT, 2021b).
Forensic readiness	Partially, some of the forensic readiness practices related to incident monitoring and incident response training are specified (see (DoT, 2021e), security control N° 27 and 142)
Incident Handling	Integrated (see (DoT, 2021e), security control N° 144)
Laws & regulations	In addition to compliance to the laws and regulations in the associated region jurisdiction and at federal level too, the ARC-IT provides specification of process that reports violations to Law Enforcement Agencies (see (DoT, 2021e), "Provide Law Enforcement Allocation").
Hardware & Software requirements	Integration of many software and hardware requirements related to the ARC-IT multiple classes of physical objects (center, field, vehicle, ITS, Personal and Support) (see (DoT, 2021e).
Industry specific requirement	Integration of many specific requirements related to either the communication or physical objects, details are provided in the associated ARC-IT communication and physical views
Security	Integrated (see (DoT, 2021d)).
Privacy	Integrated (see (DoT, 2021e) ITS communications Privacy Protection functional object).
Resiliency	One of the goal of the (DoT, 2021e) is to improve the resiliency and the reliability of the surface transportation system (see (DoT, 2021c).
Requirements Engineering	
Stakeholders identification	The ARC-IT identifies 16 stakeholders (see (DoT, 2021e), methodology).
Stakeholder concerns	The ARC-IT identifies concerns related to missions, performance, interfaces, functionality, security, organization/resources, feasibility, risks, evolvability/flexibility, deployability and maintainability (see (DoT, 2021e), methodology).
Roles identification	The (DoT, 2021e) Enterprise view defines 12 user roles.
Requirement engineering activities	Present and required as stated in the ARC-IT System engineering processes (see (Team, 2007a)).
Architecture definition	The ARC-IT is based on the <i>Systems and software engineering — Architecture description</i> 2015 architecture description standard.

Table 6.6. Mapping between the ARC-IT properties and the proposed framework.

Table. 6.6 provides a mapping of the ARC-IT proprieties and the proposed framework's attributes (General guidelines, key factors and best practices, system life cycle, requirement engineering, architecture definition, and validation & verification). It reveals the following aspects:

1. All the elements of the proposed framework are present in the ARC-IT architecture and associated documents;
2. The proposed key factors are also integrated, with the exception of the forensic requirements that are partially present in the incident handling concerns;
3. ARC-IT also considers "*Safety*" which is a major issue in ITS. However, as stated in Section. 6.2.2.2, we do not consider safety or medical concerns given that we aim to propose a more generic FbD framework, and these concerns are either industry-specific or domain-application related;
4. Some requirement engineering activities, such as requirements identification, elicitation, and analysis have not been detailed in this mapping, as more indications are already available in DoT, 2021e associated documents.

Finally, the hypothetical scenario described in Subsection. 6.4.1 is still accurate. In fact, a federal emergency or hazard monitoring system may benefit from data gathered from all the regional ITS. In this case, a Cloud computing system, as the one described in this hypothetical case study, may be required (see Figure. 6.2).

Now, let us discuss the potential opportunities and limits of the proposed framework.

6.5 OPPORTUNITIES AND LIMITATIONS

Achieving forensic-ready systems is ultimately feasible with the adoption of the System Engineering approach. As shown in the proposed framework, the efficiency of Forensic-by-design is tightly linked to: (1) a precise knowledge of the system's structure, (2) an iterative and recursive application of SE processes with a proper integration of the proposed key factors, and (3) reliable verification and validation.

The proposed framework may, therefore, benefit from: (1) SE approach efficiency, (2) knowledge of proven SE related works, studies, and experiences, (3) taking into account learned lessons from SE projects. As for the Forensic requirements integration, there are opportunities in adapting the previous efforts that have been deployed in both security engineering and privacy engineering to advance this topic.

Nonetheless, the proposed framework is a generic one and is not tied to a specific domain. Indeed, even though the newly adopted key factors (security, privacy, and resiliency) resulted from a mapping between CF challenges and previous FbD framework key factors, they are still generic and may thus be adopted for other systems.

As discussed through this chapter, there are many opportunities that may emerge from the proposed framework even if there is no real-world evaluation for now. Moreover, as for the

Rahman, Glisson, et al., 2016 framework, the proposed one also exhibits some limitations. For instance, the continuous monitoring cannot be envisioned beyond the system (or software) boundaries, unless clear and abiding agreements are established. Even so, the soundness of the evidence collection process and the admissibility of the evidence depend on the trustworthiness of the agreement signatories. Furthermore, this continuous monitoring becomes more complex when the desired system spans across multiple jurisdictions. So, as stated in the formulated hypothesis, there is still at least a category of Cloud systems (see Figure. 6.2 and 6.3) where even the proposed framework may not be efficient.

6.6 SUMMARY

Our primary hypothesis was that (a) FbD is not effective for some open boundaries systems, and (b) this strategy is not fully aligned with systems and software engineering standards. In this chapter, we wanted to confirm the stated hypothesis in the previous chapter. We adopted a research methodology which includes a mapping between Cloud Forensics challenges and FbD key factors. The emergence of persistent Cloud Forensics challenges proves that there is at least a category of open boundaries systems for which the FbD strategy may not be efficient, and points out the need for adding 3 new key factors. Moreover, the analysis of previous frameworks shows that they miss some key characteristics such as the system's structure and therefore confirms the second part of the hypothesis.

We, then, aimed to fix some of the observed insufficiencies by, first, adding 3 new key factors and specifying for each one of them their associated best practices and standards. Then, we proposed a new Systems Engineering driven Forensic-by-design framework by specifying its major guidelines, key factors, system life cycle and system development life cycle processes (such as, requirements engineering, architecture definition, validation, and verification). Finally, we proceeded to the validation of the proposed framework with a case study and an analysis of a real-world project. The next chapter is dedicated to in-depth study of the opportunities and challenges that may emerge from a forensic-ready ITS.

A FORENSIC-READY INTELLIGENT TRANSPORTATION SYSTEM

7.1	Introduction	75
7.2	Economic Impact	75
7.3	Security and Incidents	76
7.3.1	Attackers	76
7.3.2	Attack vectors and surface	77
7.3.3	Real world attacks	79
7.4	ITS DFR	82
7.5	Architecture & Standards	82
7.5.1	Selected Architecture	83
7.6	FR-ITS Opportunities	85
7.6.1	Methodology	85
7.6.2	Forensic-by-design	86
7.6.3	Concerns	86
7.6.4	Readiness	86
7.7	FR-ITS Challenges	87
7.7.1	Boundaries	87
7.7.2	Digital vs Physical	87
7.7.3	Requirements elicitation	88
7.7.4	Scale and volumes	88
7.7.5	Standards and practices	88
7.8	Summary	89

7.1 INTRODUCTION

In this chapter, we investigate the feasibility of a forensic-ready [ITS](#). Starting from its economic impact, we perform an analysis of its associated security aspects and vulnerabilities. Second, we provide a review of some real world projects and standards. Finally, we discuss the emerging opportunities and challenges from adopting a [DFR](#) standard with an [ITS](#) architecture.

7.2 ECONOMIC IMPACT

The economic impact of transportation is not to be demonstrated. In fact, transportation is present in every single aspect of citizens daily life. From travelling to goods and merchandise

delivery, the transport sector is a central nerve to a national economy. Thus, it is not astonishing to observe the symbiosis between this sector and the technological evolution in other domains leading to the emergence of concepts such as Smart cities and Intelligent Transportation System (ITS).

The ITS takes its origin from the USA in the 20th century (Alam, Ferreira, and Fonseca, 2016; Meneguette, Grande, and Loureiro, 2018), but it is gaining worldwide attention nowadays. Several projects and architectures have emerged from conjoint efforts of both government bodies and researchers (Canada, 2021; DoT, 2021e; ETSI, 2021).

In fact, the critical nature of ITS, and the diversity of its ecosystem (components, technologies, stakeholders, etc.) have led several countries to deploy efforts towards the standardization and the development of associated architectures (Meneguette, Grande, and Loureiro, 2018). Therefore, there is abundant work issued from governmental agencies and researchers, such as the ARC-IT (USA) (DoT, 2021e), the ITS architecture for Canada (Canada, 2021), and Europe (ETSI, 2021; Sjöberg et al., 2017). Moreover, the evolution of communication technologies, sensors and computation, in addition to customers needs has led to the emergence of a subset of ITS namely Cooperative Intelligent Transportation System (C-ITS) that takes advantage of the communication and cooperation between its participants (Alam, Ferreira, and Fonseca, 2016).

Finally, from the economic perspective, the ITS global market size is predicted to grow from \$1643.8 million in 2018 to \$8474.2 million by 2026 (Insights, 2021). Multiple countries are already investing in the deployment and the maintenance of these critical infrastructures. For example, the U.S is already investing more than \$25 billion in deployed ITS. The economic and societal usage of ITS by American travellers is exceeding \$2.3 billion annually (Chan-Edmiston et al., 2020).

7.3 SECURITY AND INCIDENTS

Even if there is a significant advancement in ITS research, there are still several challenges and open questions. For example, security, privacy, resiliency and safety are among the ITS concerning issues (Ganin et al., 2019; Kelarestaghi et al., 2018; Lamssaggad et al., 2021). As for security, an ITS is exposed to at least three attack vectors (physical, network and wireless) (Huq, Vosseler, and Swimmer, 2017), and multiple types of attackers.

In the following, we will discuss ITS: (1) attackers and motives, (2) attack vectors and surface, and (3) past cyber attacks and security incidents.

7.3.1 Attackers

Attackers' motives vary from money, revenge, protest, etc. Authors in Huq, Vosseler, and Swimmer, 2017 identify the following threats and attacks' perpetrators:

1. **Nation States.** Developed and developing countries may gather intelligence using dedicated software and malware, either by official teams or by outsourcing this hacking

activity to third parties such as criminal gangs. The main motive for this kind of attackers is either to steal intellectual property or to sabotage another country's ITS infrastructure in case of war.

2. **Criminal gangs.** Mainly motivated by monetary gain, this category of attackers may use ransomware and other phishing mechanisms to generate illicit revenues. Additionally, they may also be hired by a national government for various cyber attacks.
3. **Hacktivists.** Concerned by their political views, this kind of attackers use cyber attacks to draw attention to their political causes. ITS resources such as digital message boards are frequent target of these attackers to protest for multiple causes related to environment, politics, corporate greed, etc.
4. **Cyber-terrorists.** As stated by Huq, Vosseler, and Swimmer, 2017, the main motive of cyber-terrorists is to disrupt ITS services causing physical destruction and may be loss of life.
5. **Insiders.** Interns acting —directly or indirectly— against their own organisation, and therefore against themselves, their motives may vary from revenge, ideology, politics, money and ego.
6. **Unscrupulous operators.** Drivers (regulars or commercial) are the main operators in an ITS, therefore it is possible to imagine a scenario where an operator tries to abuse the system in order to save on fines, fees or to sabotage another competitor.
7. **Natural disasters.** The last threat to an ITS may be naturally caused by nature itself. Indeed, natural phenomenas, such as earthquakes, flooding, snowfall may disrupt the functioning of an ITS and may cause physical damage and loss of life.

7.3.2 Attack vectors and surface

After an in-depth analysis, Huq, Vosseler, and Swimmer, 2017 concluded that ITS are exposed to three overlapping attacks categories: physical, networks and wireless as shown in Figure. 7.1.

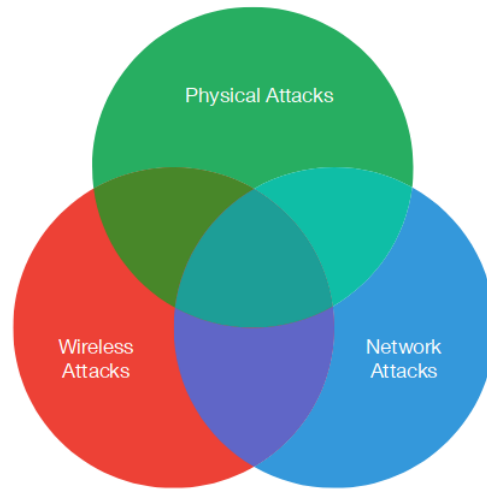


Figure 7.1. ITS security attack vectors (Huq, Vosseler, and Swimmer, 2017).

The physical attacks category is due to the fact that an ITS physical infrastructure's resources are exposed on roadways and roadsides which make them vulnerable. In fact, physical access to those resources may lead to the following attacks:

1. Physical connection to an exposed port,
2. Guessing a device credential through brute force,
3. Sniffing a network between a device and a backbone,
4. Scanning and discovering a closed network topology,
5. Deleting files on compromised ITS devices, etc.

Above are some of the potential ITS physical attacks. A complete list of 14 potential physical attacks is listed in Huq, Vosseler, and Swimmer, 2017.

Networks are already vulnerable to multiple attacks. Moreover, internet exposed ITS networks, and IoT based systems are particularly vulnerable to cyber-attacks. This category of attacks contains threats such as:

1. Identifying and abusing device misconfiguration,
2. Remote system discovery and abuse,
3. Uploading and installing malicious firmwares,
4. Social Engineering attacks,
5. SQL injections, etc.

In addition to the above cited attacks, Huq, Vosseler, and Swimmer, 2017 identified a total of 21 ITS potential network attacks.

Finally, the wireless attacks emerge from vulnerabilities that may exist in an ITS subsystem such as Vehicle to Vehicle (V2V), among these attacks —11 attacks as broughten by Huq, Vosseler, and Swimmer, 2017— we may cite:

1. Sniffing wireless transmissions,
2. Remote hijacking of vehicle,
3. Electronic jamming,
4. Man in the middle attacks,
5. Exploiting vulnerabilities in software, hardware, and protocols, etc.

ITS cyber attack are not a matter of speculation any more. In fact, they are already taking place. In the following subsection, we provide some ITS cyber attack and security incidents.

7.3.3 Real world attacks

Multiple ITS real-world attacks have taken place in the last years ranging from road sign hack (Kelareshghi et al., 2018) to ransomware attacks (Huq, Vosseler, and Swimmer, 2017). More recently, some major Metropolitan Transportation Authority's computer systems were the target of cyber crime (Inquirer, 2021; Times, 2021). In the following, details on these attacks.

7.3.3.1 Road sign attacks

Variable Message Sign (VMS) and Traffic Signal Controllers (TSC) are among major ITS infrastructure (Kelareshghi et al., 2018). If hacking of road infrastructure was a rare event in the past, it becomes more frequent recently. As shown in Figure. 7.2, a VMS is vulnerable to physical access attacks, such as in the context of Figure. 7.2. For example, a group of students from MIT hacked a VMS to display the following message “*This sign has been hacked*”.



Figure 7.2. Sign hack (Kelarestaghi et al., 2018).

Kelarestaghi et al., 2018 made an in-depth risk analysis of VMS threats, established an attack tree and listed some of the system vulnerabilities. Additionally, the authors provide an exhaustive list of recent VMS attacks.

Even if VMS attacks may seem benign, they may become worse either by the display of offensive messages or by disturbing ITS traffic through drivers distraction. Kelarestaghi et al., 2018 conclude that for now VMS hacking may cause traffic slowdown, threaten road users' safety, and cause financial loss. However, crashes, fatalities and public chaos are among the possible outcomes of this type of ITS security attacks.

7.3.3.2 Ransomware attacks

Ransomware attackers main motive is purely lucrative (money). Indeed, upon the infection, the ransomware encrypts the victim's data and attacker asks for payment in order to decipher the encrypted data. Beyond fears of personal data leakage and privacy breach, this kind of attack may render an ITS out of service and therefore disturb the whole system functioning. As stated in Huq, Vosseler, and Swimmer, 2017, in 2017 a ransomware attack on Washington police department surveillance camera networks impacted their ability to record for three days. More recently, an attack on a Metropolitan Transportation Authority (MTA) timekeeping systems (see Figure. 7.3) has led to a service outage that lasted several days causing for sure financial loss.



Figure 7.3. M.T.A time keeping systems ransomware attack (Nypost, 2021).

7.3.3.3 Remote Car Hijacking

Probably one of the most alarming types of attack, remote car hijacking is not a matter of speculation. In fact (Miller, 2019) have already provided a proof of concept of a remote car hijacking (see Figure. 7.4).



Figure 7.4. Remote Car Hijacking (Miller, 2019).

In their experience, the author after taking remotely control of the car, they proceeded to manoeuvre the steering wheel and tow it to a ditch.

Certainly, ITS cyber-attacks and security incidents are very alarming. Beyond the financial loss that they may cause, physical harms and fatalities are the most feared. However, the worst scenario is the hypothesis of an attacker having the ability to conduct a cyber crime in an ITS infrastructure in order to disguise a crime as an accident.

In the following section, we discuss the required capabilities for an ITS that will enable it to conduct a sound DFI with minimal cost and service disruption.

7.4 ITS DFR

Incidents and cyber crimes happen. In the following, we investigate the ITS due forensic readiness (*i.e., enhance the ITS with capabilities that ease the collection of digital evidence with a minimum disruption and less economic impact from a potential investigation*). So, for this purpose we adopt the following methodology:

1. Define clearly what we mean by enabling an ITS with the due DFR capabilities. And more precisely, what is a “forensic-ready” ITS.
2. Select a candidate ITS architecture.
3. Assess the opportunities and challenges that may emerge from either enabling an ITS with the due DFR capabilities or design and develop a “forensic-ready” ITS.

As for the first question, we either opt to ensure the due DFR capabilities at the “Production” stage, or aim towards the design and development of a “forensic-ready” ITS. Elements of response for this question have already been stated in Chapter. ?? (see Subsection. 6.4.2). Therefore, in this chapter, we will aim towards the design and development of a Forensic-Ready Intelligent Transportation System (FR-ITS).

In regards to “Forensic-ready”, we in here define it as a system (or software) state that is associated with the system (or software) ability to collect digital evidence whilst minimizing the costs of an investigation and disruption of business, and which is related to a specific period of time along its life cycle.

In fact, a system (or software) may be engineered (designed and developed) to be forensically ready at the design and development stage by adopting the Forensic-by-design strategy, and continue to be *Forensic-ready* along its life cycle by allocating the required digital forensic readiness capabilities at the production, support and retirement stages. Thus, “Forensic-ready” is a temporal state (propriety) of a system (software).

The following section provides details on the selected ITS architecture.

7.5 ARCHITECTURE & STANDARDS

In this section, we introduce the selected ITS architecture, provide details on its different stakeholder, viewpoints, views, and security capabilities, then present the incident investigation

principles and processes standard (*Information technology — Security techniques — Incident investigation principles and processes 2015*).

7.5.1 *Selected Architecture*

Among the ITS architectures cited in Section 7.1, the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) (USA) (DoT, 2021e) is the most advanced and maintained. In fact, the ARC-IT architecture was first initiated in 1996 and is still maintained and updated, even the ITS for Canada (Canada, 2021) is in a re-alignment process with it. Moreover, the U.S. Department of Transportation is licensing all the ARC-IT architecture documents and resources under the public domain license. For the conjugate of the above arguments, we opted for this architecture.

The methodology behind the ARC-IT is encapsulated in the fact that: “a system has an architecture, stakeholders have interests and concerns in a system. So, the architecture viewpoints frame the concerns and the architecture views address those concerns”. The distinction between viewpoints and views is of importance in the ARCT-IT. The group of stakeholders considered in this architecture is composed of: Federal government, state/local government, Non-profit/advisory, private sector and general public. Stakeholders’ concerns and interests dictate the architecture viewpoints, therefore, as depicted in Figure 6.6, the ARC-IT is composed of four views: (1) Enterprise, (2) Functional, (3) Physical, and (4) Communication.

7.5.1.1 *Enterprise viewpoint*

The Enterprise viewpoint considers the policies, funding, agreements and jurisdictional structure; Provides a basis of ITS understanding for implementers and specifies their roles; Specifies the objectives and goals for the surface transportation system; Provides the policies and process to support transportation planning and project development. Additionally, it answers stakeholders potential concerns on roles and relationships. In fact, ITS involved groups may have roles that vary from installation, maintenance, providing applications or devices, providing transportation-related user services, etc., therefore, creating an ecosystem of multiple providers and consumers, where relationships must be enumerated in a concise manner. In association with the Enterprise viewpoint, the Enterprise model provides details on concepts, such as Enterprise object, resource, role and relationship.

7.5.1.2 *Functional viewpoint*

The Functional viewpoint provides an abstraction of the physical viewpoint to ease the task of potential application, device or service developers’. For this purpose, the Functional view comprises a set of abstract functional elements and their logical interactions, therefore answering potential developer questions on required data format and functionalities for a given service without bothering with the physical details at this layer. On the other hand, the ARC-IT

Functional model is developed using a Structural Analysis methodology and uses some structural analysis artefacts, such as process, process specification (p-spec), data flows, and terminators. Finally, the ARC-IT (DoT, 2021e) specifies that: “The Functional View defines Processes to control and manage system behaviour, such as monitoring, and other active control elements that are part of describing the functional behaviour of the system”.

7.5.1.3 Physical viewpoint

The physical viewpoint is an engineering viewpoint that describes physical elements and enables engineers to answer questions about involved physical elements in a given delivered service, their interfaces, exchanged information, security consideration, etc. Therefore, it defines objects, such as physical objects (P-Object) (Center, Field, Support, Personal, Vehicle), Functional Object, Information flow, Triple, Subsystem, Terminator and Service Package Diagram.

The physical view comprises a set of physical objects (sub-systems and terminators), that are categorized in six different classes. A general ITS class that covers all of ITS, while five more specific classes (Center, Field, Support, Personal, vehicle) as shown in Figure 7.5.

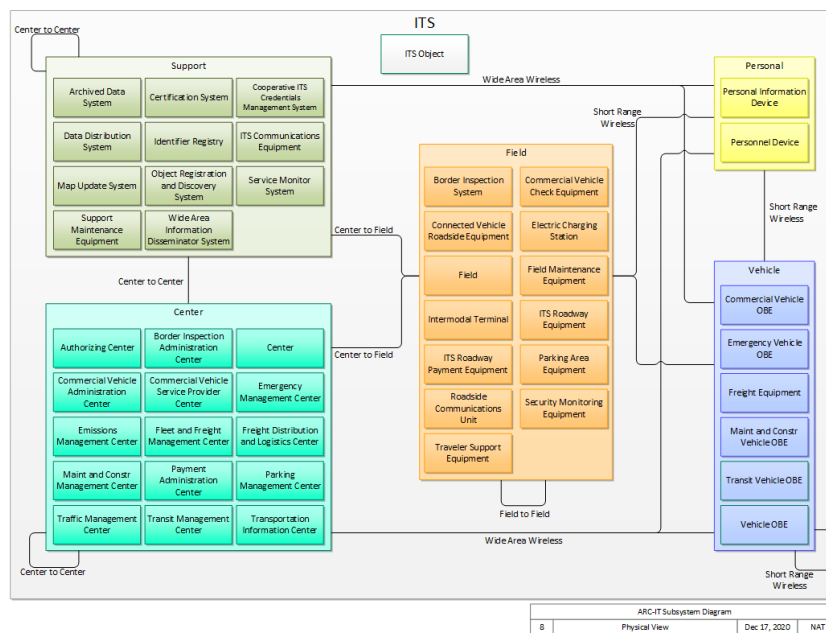


Figure 7.5. The ARC-IT Physical view (DoT, 2021e).

The ARC-IT specifies that: “The general ‘ITS Object’ includes core capabilities common to any class of object”, thus making it an abstract object from which all the objects of other classes derive. Therefore, this object “includes the core capabilities and interfaces that may be included in any ITS system or device”.

7.5.1.4 Communication viewpoint

The communication viewpoint provides a set of protocols that enable the communication between physical objects. Thus, this viewpoint specifies a set of requirements, such as performance, interoperability, security, etc. Additionally, it comprises a set of environment and operational challenges associated with existent policies and regulations. Therefore, it aims to provide answers to potential engineers' questions. The ARC-IT communication model comprises a set of layers; Access layer, TransNet layer, Facilities Layer, and ITS Application layer. Moreover, it also provides a mapping with the OSI model, IETF IP Suite, NTCIP model, etc. To prevent the disruption and the alteration of ITS operations, the ARC-IT includes security measures that address some security aspects, such as information security, ITS personal security, Operational security and security management. The aforementioned security axes are enclosed in the "*Securing ITS*" capabilities, however, the ARC-IT defines eight areas for security compliance; Disaster Response and Evacuation; Freight and Commercial Vehicle Security; HAZWAT Security; ITS Wide Area Alert; Rail Security; Transit Security; Transportation Infrastructure Security; and Travellers Security.

While studying the ARC-IT, it seems that it does not offer any capability to address or support a potential digital forensic investigation. However, the conjugate of this architecture and the incident investigation principles and processes (see Chapter. 3, Section. 3.3.3) is a promising venue for a Forensic-ready ITS.

In the following section, we investigate the emerging opportunities from this perspective and potential challenges and issues.

7.6 FR-ITS OPPORTUNITIES

Enhancing an ARC-IT based ITS with the due forensic capabilities imply ultimately the update of the architecture itself. In fact, the ARC-IT is based on the ISO/IEC 42010 (*Systems and software engineering — Architecture description 2015*) architecture description standard.

7.6.1 Methodology

One of the major advantages of the ARC-IT is the fact that it is based on the (*Systems and software engineering — Architecture description 2015*) architecture description standard, which offers the flexibility to start from stakeholders' concerns and interests, establish different viewpoints, and provide associated views. Furthermore, it allows different scales of implementation, going from a local ITS to regional one. Moreover, it is also aligned with the systems and software engineering and adopts the "V" system engineering model (Team, 2007b).

7.6.2 Forensic-by-design

Similar to “Security-by-design”, the “Forensic-by-design” (Rahman, Glisson, et al., 2016) paradigm suggests the integration of the forensic requirements at the earliest phases of a system’ design and development stages aiming for a Forensic-ready system by essence. To the best of our knowledge, among the six key factors of the Forensic-by-design framework (*i.e. Risk management principles and practices, Laws and regulations, Forensic readiness principles and practices, CPCS hardware and software requirements, Industry-specific requirements, Incident handling principles and practices*) only the forensic readiness principles and best practices is missing in the ARC-IT architecture. However, there is an opportunity to integrate this key factor at the design and conception of an ITS by updating the ARC-IT architecture as explained in the following subsections.

7.6.3 Concerns

One of the major key elements in the ARC-IT methodology is the enumeration of stakeholders’ “concerns”, such as performances, interfaces, security, risks, personal (safety, privacy), deployability, etc. Thus, conciliating the stakeholders’ concerns and needs with the forensic requirements is a necessity. This may be achievable through the elevation of awareness about potential real world incidents that may be caused by digital incidents (Miller, 2019). Once the level of awareness is attained, the integration of forensics requirements into the architecture will be feasible.

7.6.4 Readiness

In the ISO/IEC 27043:2015 standard, the readiness processes group contains indications on the proper methodology to prepare before an incident happens.

The *Scenario definition* process imposes the enumeration of all the scenarios in which digital evidence is required. For ITS scenarios, such as road signalization hack (Kelarestaghi et al., 2018), remote car hacking (Miller, 2019), and attacks on MTA (Inquirer, 2021; Times, 2021) may be envisioned. More general scenarios may be derived from the analysis of potential ITS surface attacks. Thus, supposing the compromise of any ITS subsystems, terminator, object (physical, communication, functional) will lead to a scenario worth investigation.

Once the scenario is defined, the enumeration of digital evidence sources is next. For this purpose, the inventory of all potential sources within all the ITS sub-systems is required. In fact, potential evidence may lay inside physical and communication objects, and especially the ITS object which is considered as a template for other objects. Afterwards, the planning of evidence collection and storage will for sure induce changes in the physical, communication and functional objects, in addition to the emergence of new data flows related to evidence handling and storage. Finally, the ARC-IT may be updated to contain a sub architecture related

to the ITS forensic readiness. Even if there are promising opportunities to add forensic readiness to the ARC-IT in order to obtain a Forensic-by-design ITS, there are still some concerning challenges that may undermine the feasibility or the implementation of such type of ITS, in the following some of these challenges.

7.7 FR-ITS CHALLENGES

In the following some of the most important challenges that may impact the feasibility of a Forensic-Ready ITS.

7.7.1 *Boundaries*

An ITS is delimited by geographic and service boundaries. Therefore, the aggregation of services, data, and resources to investigate a potential incident that may occur outside the ITS borders is problematic. In fact, this challenge is more related to the multi-jurisdiction issues that may emerge. Additionally, the ARC-IT comprises “*Terminators*” (e.g. financial institution, weather service, and enforcement center) that are physical objects but peripheral to the ARC-IT environment and do not contain functional objects. Even if, “*the ARC-IT shows interfaces to and from these supporting or external physical objects but does not define functionality*”. Thus, in case of a cyber crime within the ITS boundaries (e.g. Remote vehicle hack (Miller, 2019) leading to a crash), the ARC-IT contains the capabilities to detect the incident, clear the way for the emergency services, transmit the related incident data to the associated Law Enforcement Agency, but still the conduct of a potential digital investigation on the perpetuated cyber crime is considered outside the scope of the ITS. The hypothesized scenario may become more complex if the remotely hijacked vehicle crash happens outside the geographic ITS’ boundaries.

7.7.2 *Digital vs Physical*

Security is one of the ARC-IT stakeholders’ concerns. However, incidents are viewed primary from the perspective of physical and concrete assets rather than information perspective. In fact, incidents monitoring and detection in this architecture are related to traffic management, disaster response and evacuation, alert system, etc. So, securing the physical object and data flow by using devices to detect and monitor “real world” incidents derive from the analysis of scenarios where incidents are caused and initiated by an attack on physical assets rather than those which are caused by the exploitation of a digital vulnerability. For example, while investigating a multiple vehicle collision, investigator attention may be centred on conduct misbehaviour, traffic violation. However, it may also be caused by light signalization hack. Therefore, the focus on the physical incident may mislead the investigator about the origin of the incident.

7.7.3 *Requirements elicitation*

Even if the ARC-IT specifies stakeholders concerns, users needs, sub-systems and services packages requirements, to the best of our knowledge there is no mention of forensic requirements. As stated in potential opportunities, if the forensics concerns are considered then maybe there will be elicitation of its associated requirements.

7.7.4 *Scale and volumes*

The implementation of an ITS induces a large scale deployment of sensors and actuators. In fact, the ARC-IT physical view contains multiple objects (subsystems, terminators), and each system may require a set of sensors employing different technologies and which are allocated to different missions. For example, the Security Monitoring Equipment (class: field), contains a set of sensors dedicated to tasks, such as providing information on equipments security and fault indication, environment threats (e.g., chemical agent, toxic , biological, explosives and radiological), motion and intrusion detection, objects detection (metal), etc. In addition to sensors, there are also equipment and systems on vehicles, personal, centers and support physical classes. Therefore, the aggregated data type is heterogeneous (text, images and videos), often in different formats, and voluminous. In addition to the aforementioned constraints, the nature of the ITS dictated a real time data processing, at least for traffic incident monitoring. These difficulties may urge the usage of paradigms such as cloud computing and fog computing. However, digital forensic readiness and investigation models in these two domains do not yet gain maturity and are still an ongoing research.

7.7.5 *Standards and practices*

While studying the ARC-IT, it appears that there are no standards associated with multiple physical objects, such as security monitoring equipment, vehicle OBU, emergency telecommunications system, alerting and advisory system, etc. In addition to the lack of standards, vehicle forensic investigation is very challenging (Le-Khac et al., 2020; Kopencova and Rak, 2020) in many aspects, such as vehicle constructors obfuscation of technical details, digital evidence collection issues, lack of vehicle digital evidence acquisition and analysis tools, and the need for a sound forensic investigation approach. Finally, one most important issue is related to the first responder and LE training (Holt and Dolliver, 2021), and their ability to recognize the necessity of digital forensic and to properly acquire, collect and handle digital forensic evidence on-scene, such ability is strongly required in case of a fatal vehicle crash.

7.8 SUMMARY

The ITS is part of a smart city and a pivotal element of an economy. The growth of ITS associated market size, the diversity of devices providers, government funding either in development, deployment are clear indicators of the effervescence it generates. Considered as a critical infrastructure, the ITS involves several stakeholders that have interests and concerns. Even if there are concrete advances in this field, there are still some concerns related to security, privacy, resiliency and safety. Incidents and cyber crime are no matter of speculation. In fact, ITS are already targets of cyber attacks going from ransomware to road signs and remote car hacks.

In this chapter, we investigate the feasibility of a Forensic-ready ITS, more precisely, we aim to analyse the opportunities and challenges that may arise from enhancing an existing ITS architecture with the due forensic readiness capabilities in order to ensure a designed forensic ready ITS. For this purpose, we provided details on the ARC-IT which is an ITS reference architecture, and the investigation principle and process standard.

Even if there are some promising opportunities associated to the flexibility of the ARC-IT and the digital forensic readiness processes, there are still some challenges related to the ITS boundaries, the necessity to reconsider the balance between the digital vs physical aspects of an incident, the complexity of an ITS, the generated data volume, and finally the lack of standard and best practices.

Nonetheless, we believe that there are real opportunities to achieve a Forensic-ready ITS if only and only if there is a stakeholders' awareness on the possibility of exploiting a digital vulnerability to endanger traveller's safety.

In the second part of this thesis, we first investigate some of the [CF](#) legal challenges, more precisely the cross-border digital evidence access, and law enforcement request management. Second, we propose a Cloud Law Enforcement Request Management System (CLERMS).

LE EVIDENCE ACCESS IN THE CLOUD

8.1	Introduction	90
8.2	Multi-jurisdictions	91
8.3	Formal channels for cross-borders data access	91
8.4	Transparency reports and LE guidelines	92
8.5	LE requests management system	93
8.6	Legal request processing Issues	94
8.7	Problem statement	95
8.8	Goals and Scope	96
8.9	Summary	96

8.1 INTRODUCTION

Major cloud service providers (CSPs) are legally domiciled in the USA, but do have subsidiaries around the world (Facebook, 2020a; Google, 2020c). CSPs consumers, data, and partners are by de facto scattered around the globe. For example, a Spanish users' data may be stored in a USA datacenter and processed through an Irish facility. Therefore, data localization is a challenging issue especially in case of incidents or cybercrimes.

Moreover, law enforcement (LE) access to digital evidence depends entirely on the CSPs trustworthiness and the complexity of the associated legal procedures (Manral et al., 2020; T-CY, 2020a). In fact, CSPs' LE guidelines point out the need to foreign LE to address their requests through formal channels such as the Mutual Legal Assistance Treaty (MLAT) (Funk, 2014). The assertion of a jurisdiction during an investigation —*in some instances*— is problematic. In fact, even if the LE is domiciliated in the same jurisdiction as the CSP, the potential digital evidence may be located overseas, and require cross-borders data access mechanisms (Google, 2017; Mulligan, 2018; D. Svantesson and Gerry, 2015).

The multi-jurisdictions issue is one of most persistent Cloud Forensic (CF) challenges (Herman et al., 2020; Manral et al., 2020; Ruan, Carthy, T. Kechadi, and Crosbie, 2011; Simou et al., 2016). Nowadays, CSPs are being tired between domestic and foreign legislations (Google, 2017). There is an abundant literature on the multi-jurisdictional issues (Abraha, 2019; Daskal, 2018; Koops and Goodwin, 2014; D. J. B. Svantesson and Zwieten, 2016; Walden, 2012). However, the existent propositions focus mainly on the legal standpoint, because it is primarily a legal challenge.

8.2 MULTI-JURISDICTIONS

Cloud computing elasticity induces data localization challenges. In fact, data may be stored, processed, and mirrored across multiple jurisdictions. As for data, Cloud services are also consumed by users across the globe. Multi-jurisdictions in its simplistic form may be sketched as follow: *How may a Spanish LE agent investigate a cybercrime against Spanish victims committed by a USA cybercriminal resident in the UK, where the potential evidence is stored in Ireland, and processed in Asia region data centers that belong to a USA domiciled CSP?*

Furthermore, the multi-jurisdictions challenge goes beyond the territoriality, or nationality of customers and providers. In fact, from a legal perspective, a “Jurisdiction” may take at least three forms as stated by D. Svantesson and Gerry 2015, pg.3.

In the case of cross-borders investigations, international law experts specify two forms of cooperation —“*formal channels*” and “*informal channels*”— between a foreign LE and a CSP (Koops and Goodwin, 2014; Walden, 2012). Additionally, Walden, 2012 formulated four possible courses of action for foreign LE (Walden, 2012, pg.55). Even so, major CSPs are still restricting foreign LE requests to the formal channel through Mutual Legal Assistance Treaty (MLAT) or Rogatory letter.

8.3 FORMAL CHANNELS FOR CROSS-BORDERS DATA ACCESS

There are three formal channels for cross-borders data access: (1) Mutual Legal Assistance Treaties (MLATs) (Funk, 2014), (2) Rogatory letters, and (3) the Clarifying Lawful Overseas Use of Data (CLOUD) act (U.S.A DOJ, 2018, 2020). While the two first mechanisms have been there for decades, the last act was enacted in March 2018.

The MLAT channel is primarily used by LE, and the Rogatory letters are often used by non-government litigants (see Funk, 2014, pg.5, pg.17). Even if the MLAT process is theoretically simple (see Lin and Fidler, 2017, pg.2), in practice it faces challenges (as shown in Figure. 8.1), such as procedure complexity, processing latency, guideline issues, and requests processing capacity (USA DOJ, 2014; James and Gladyshev, 2016; T-CY, 2020b; Woods, 2017).

Finally, the CLOUD act aims to address some of the MLATs inefficiencies and speed up the access to digital evidence (see Bilgic, 2018, pg.333). In fact, it authorizes bilateral agreement between the U.S.A and a *trusted* foreign partner to obtain direct access to digital evidence, wherever they are located. However, eligible foreign countries must meet some requirements such as the protection of privacy and civil liberties during the data-collection activities. In fact, the “*trusted foreign partner*” condition has some political ramifications. As for now, only some countries such as the U.K have gained benefit from this mechanism. Moreover, there are several research works discussing the impact of this new legislation on the existent formal channels, privacy, and international laws (Abraha, 2019; Daskal, 2018; Mulligan, 2018).

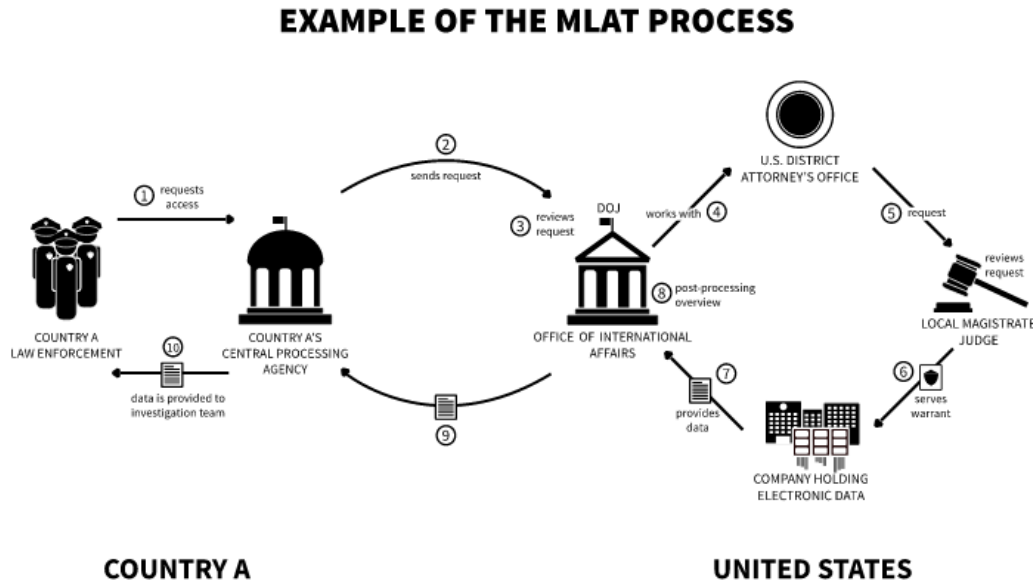


Figure 8.1. Example of an US MLAT process for Electronic Evidence (Lin and Fidler, 2017).

8.4 TRANSPARENCY REPORTS AND LE GUIDELINES

A [LE](#) request may vary from disclosure, preservation, removal, and testimony. On counterpart, CSPs may approve, reject or even challenge a request (Fondation, 2015; D. Svantesson and Gerry, 2015). CSP's response to received LE requests is mainly based on: (a) domestic jurisdiction laws, (b) regulations, (c) internal policies (Facebook, 2020b; Google, 2020d), (d) associated legal procedure, e.g., *Subpoenas*, *Court orders*, *Search warrants*, etc. (Yahoo, 2020), and (f) the request status (emergency or not). In fact, emergency requests are handled promptly, and processed with the due priority (Amazon, 2021; Facebook, 2020b).

Approved LE disclosure requests may lead to the communication of either “*Non Content Data*” or “*Content Data*”, if available data is found for the request's stated period (Amazon, 2021; Facebook, 2020b; Google, 2020d). Statistics on disclosed users' information are published in CSPs transparency reports, which are often heterogeneous. In fact, only Microsoft (Microsoft, 2020b) and Yahoo (Yahoo, 2020) seem to use similar formats. Additionally, CSPs also publish guidelines for LE (Amazon, 2021; Facebook, 2020b; Google, 2020d; Microsoft, 2020a; Yahoo, 2020). Table. 8.1 provides a summary of transparency and law enforcement guidelines attributes.

Transparency reports	
Attribute	Description
Volume	Number (percentage) of received requests, Users' impacted accounts, and delivered responses (accepted, rejected). In case of accepted requests statistics on " <i>content data</i> " vs " <i>no content data</i> " responses are also provided.
Requester	Type of requester authority: Law Enforcement Agency (LEA), FISA
Legal procedure	LE requests associated documents (subpoena, court order, search warrant, etc.).
Localization	Requester geographical origins, either by country or a comparison between domestic country vs. Foreign.
Status	Specification on requests regime (emergency or not).
Objective	Requested actions on target's data (disclosure, removal, preservation and testimony).
Historic	Indications on past transparency reports.
Law Enforcement Guidelines	
Legal requirements	Request legal ground of acceptance.
Emergency exception	Exceptions to the legal requirements for emergency requests.
Suited actions	Type of receivable requests, and suited actions on data. In the case of a preservation request, the associated preservation delay.
Target	Targeted user required identity (Id, Account, Email, etc.).
Target notification	Target notification policy, when and how a CSP may (or not) notify a user about an issued government request on its data.
Requester identity	Information required from a requester to show authenticity and authentication.
Submission means	Permissible means for request submission (email, mail, fax or online).
Costs reimbursement	Regime, and exception on cost reimbursement to due business disturbances and request compliance induced fees.

Table 8.1. CSP's Transparency reports and LE guidelines attributes.

8.5 LE REQUESTS MANAGEMENT SYSTEM

To the best of our knowledge, there is no previous work on law enforcement requests management systems. Certainly, major CSPs do have their own solutions to manage and process LE requests. However, LE requests pre-submission is only permitted via Fax or Email. As far as we know, only Facebook and Google (Facebook, 2020c; Google, 2020e) propose an online requests pre-submission portal for the exclusive usage of LE agents.

In the following section, we provide details on some of the law enforcement request handling challenges.

8.6 LEGAL REQUEST PROCESSING ISSUES

As stated in Section. 8.2 multi-jurisdiction is a persistent challenge in CF and more specially in cross-border data access. However, legal request processing faces also other challenges that are amplified by legal consideration, such as the following:

1. **Volumes:** There is for sure a significant growth in LE requests. For example, the number of legal requests for users' information disclosure submitted to Google raised from 165,894 in 2019 to 217,424 in 2020. If this is the current state for CSPs, the situation may be worse considering the central entity—Office of International Affairsi (OIA)—that evaluates foreign LE requests —via Formal channel (MLAT)—. Indeed, in the United States, the OIA state that:

Over the past decade the number of requests for assistance from foreign authorities handled by the Criminal Division's Office of International Affairs (OIA) has increased nearly 60 percent, and the number of requests for computer records has increased ten-fold. (USA DOJ, 2014, see page 1).

The growing number of LE requests implies a need for automation for both the responder and the central entity that evaluate the foreign request.

2. **Delays:** Latency in processing LE requests is observed in two cases: (1) At the CSPs level, in fact a request is not processed until the reception of the associated legal documents via mail, (2) in case of a foreign request via formal channel where a nine step process is enacted and which involves many instance other than the CSP (see Subsection. 8.3). The MLAT process takes from six weeks to ten months on average (Lin and Fidler, 2017, see page 3).
3. **Transparency:** The lack of transparency is observed at least in two cases: (1) Generally, CSPs do not provide any technical capabilities for LE to monitor the process flow of their submitted requests —with the exception of those that propose an online portal—, additionally, CSPs do not provide response to testimony requests, (2) Considering foreign request, formal channel procedures are so complex and involve several parties that it is difficult to monitor the handling of the submitted request. Furthermore, in case of requests leading to the collection of digital evidence, the admissibility of those collected evidence stands only on the trustworthiness of the CSPs, and may be challenged in a foreign court of law. Indeed, some researchers have already pointed out this possibility:

It is important to recognize that data obtained from a cloud-based service may be excluded from use in court proceedings on a number of grounds (see Walden, 2012, pg. 64).

4. **Procedures:** LE guidelines are mainly in English or translated into a few languages. Assisting LE in the submission process is crucial. However, CSPs do not provide detailed procedure for request submission, nor do they provide standard forms. Making assumptions on LE agents training or having the necessary training to make such a

request without any assessment may lead to submission being rejected due to error or misinformation. Foreign requests procedure are so complex that it requires for a foreign LE to have training on how to formulate request through formal channel, this is also asserted by USA DOJ, 2021:

Coordinate with OIA to develop a plan to improve its training and outreach efforts including considering the creation of an external site of resources for foreign authorities.(USA DOJ, 2021, see page 29)

As stated above, there is certainly a dependency between the legal and technical aspects of LE requests processing. The complexity of legal procedures for cross-border data access induces some technical challenges, such as latency, volume and transparency. On the other hand, the lack of automation in both the responder and the central entity (OIA) request processing induces an increase of the cases backlog and therefore latency in legal reviews of the formulated request both domestic and foreign.

The need for a scalable technical solution for LE requests processing for both responder and central entity—in case of a foreign request—is persistent. Indeed, even the OIA have expressed the need for a reform in MLAT processing and the adoption of scalable case management system (CMS) as expressed below in (USA DOJ, 2021):

Coordinate with CRM ITM to ensure OIA has access to CRM’s Oracle Apex platform and support the automation of OIA’s team trackers and leadership dashboards. (USA DOJ, 2021, see page 29).

In the following section, we describe clearly the main problem that we aim to resolve in the following chapter.

8.7 PROBLEM STATEMENT

Certainly digital evidence access in Cloud computing environments is very challenging (see Subsections. 8.2 and 8.3). Technical issues are amplified by legal aspects. If the handling of domestic LE requests seems straightforward, foreign requests in counterpart are subject to more complex procedures. Among the aforementioned challenges, trust and transparency seem to be the most difficult to resolve. Moreover, these two aspects (transparency and trust) are also required to ensure the soundness of the conducted DFI processes and the admissibility of the collected digital evidence.

After the analysis of transparency reports and LE guidelines (see Subsection. 8.4), it appears that there is a need to either maintain the current state of LE request handling—processes and associated technical capabilities— waiting for advancement in legal frameworks establishment especially in case of foreign LE requests, or anticipate the venue of these “*legal frameworks*” by designing and developing new technical capabilities that may resolve some challenges and attenuate the complexity of other ones. In fact, some major CSPs are already providing an online portal for LE request pre-submission (see Subsection. 8.5).

If CSPs process the resources needed to the design and the development of associated LE requests processing technical capabilities, other organisations (eg., Small and Medium Sized Enterprise) that are outsourcing part of their information system to a CSP may not. And, in some circumstances those organisations may be requested to respond to legal requests.

So, in abstraction of the nature of the responder (CSP or not), in the following chapter we aim to answer the following question:

What are the required technical capabilities that a responder should possess in order to handle transparently legal requests in accordance with specified guidelines, laws and regulations ?

8.8 GOALS AND SCOPE

As far as we know, there is no prior work on a cloud legal request management system. Moreover, the only existent systems are proprietary (CSP in-house made) that are for the law enforcement agents exclusive usage without any public or published documentation.

Therefore, our main motive is to establish an affordable, scalable and open source based technical solution that may ease some of the LE request handling challenges. More precisely, we are aiming towards the design and development of solution that fit any sized organisation—going from public CSPs to the smallest enterprise that is outsourcing part of its Information System (IS) to a CSP— and achieve the following:

1. Facilitate the communication between the requester and the responder and ensure a transparent request handling,
2. Provide the responder with a minimal DFR baseline to guarantee a sound DFI process and the admissibility of the collected digital evidence.

8.9 SUMMARY

In this chapter, we presented one of the most complicated [CF](#) legal challenges, and which is Multi-jurisdictions. More precisely, we focused on enhancing a responder with the due capabilities required to comply to law enforcement (foreign or domestic) requests. While not focusing on the legal aspects, we aim to provide a responder with technical modules that may ease a law enforcement handling and management. In the next chapter, we will provide an abstract architecture for a Cloud Law Enforcement Request Management System, a proof of concept and a validation scenario.

CLOUD LAW ENFORCEMENT REQUEST MANAGEMENT SYSTEM

9.1	Introduction	97
9.2	The Proposed solution	97
9.2.1	LE request processing flow	98
9.2.2	Architecture definition	99
9.2.3	System requirements	102
9.3	Prototype design & development	102
9.4	Cloud deployment	104
9.5	Prototype validation	106
9.6	Economic assessment	107
9.7	Opportunities & limits	108
9.8	Summary	109

9.1 INTRODUCTION

In this chapter, we propose a technical and organizational solution to simplify the LE request handling process. Our main objectives are: (1) to facilitate the communication between the requester (LE) and the responder, (2) ensure transparency in handling a LE request, (3) enhance the due forensic readiness capabilities of the responder.

9.2 THE PROPOSED SOLUTION

Upon statement of the main problem (see Section. 8.7), in this section, we propose a technical solution for some of the LE requests handling challenges. Therefore, we will address the following points:

1. Analysis of a LE request handling workflow.
2. Proposition of an abstract architecture.
3. Analysis of the system requirement.
4. Design, development, and deployment of a prototype.
5. Validation of the proposed system with two hypothetical scenarios.
6. Economic assessment of the associated deployment costs.

9.2.1 *LE request processing flow*

CSPs governance is based on: (1) business term of services, (2) applicable domestic jurisdiction laws, and (3) compliance to regulations and standards.

That being said, governance is also asserted through organizational policies and technical capabilities. Therefore, the specification of the internal workflow, data flow, and external partners' communication channels are vital. In this context, existent incidents response and digital forensic investigation policies may be enhanced with a new law enforcement policy that specifies the communication with LEs. Furthermore, on the technical side, the implementation of a law enforcement request management system will ease the CSP-LE communication and ensure a transparent requests processing.

Based on available CSP LE guidelines (Facebook, 2020b; Google, 2020d), a typical LE request processing work flow (Figure. 9.1) includes 3 major steps: submission, evaluation and response.

Even if there are some considerations in the processing of some LE requests (see. Section. 8.4) (e.g., an emergency request is considered as an exception to the LE guideline and is handled promptly), the above cited stages are still present and the handling particularities appear in some procedures and tasks.

Details on the LE request handling stages:

1. **Submission:** we observe that major CSPs accept only requests submitted by Fax or Email. Even if there are some CSPs that offer an online portal for request pre-submission, the effective request evaluation is only initiated at the reception of the legal documents via the mail. However, in case of emergency or preservation requests, some actions may be initiated (anticipated) in due respect to the adopted law enforcement policy.
2. **Evaluation:** upon effective reception of the request's legal documents, a team composed of law assistance, IT manager, incident response members, and forensic experts may gather to evaluate a possible response based on pre-established internal law enforcement policy. In case of approved disclosure (or preservation) requests an escalation to a full DFI is required. In such cases, collected digital evidence, chain of custody documents and other DFI reports may be included within the formal response to the requester.
3. **Response:** a formal answer is transmitted to the requester (by email or mail). Approved requests may lead to: (1) the application of the requested actions (preservation, disclosure, deletion) on the target's data, (2) notification of the target (in some cases), establishment of an invoice for the costs reimbursement. Moreover, a responder may also reject a request or even challenge it (see Subsection. 8.4). Finally, we observe that major CSPs do not respond to testimony requests and offer only a certificate in exchange for an expert testimony.

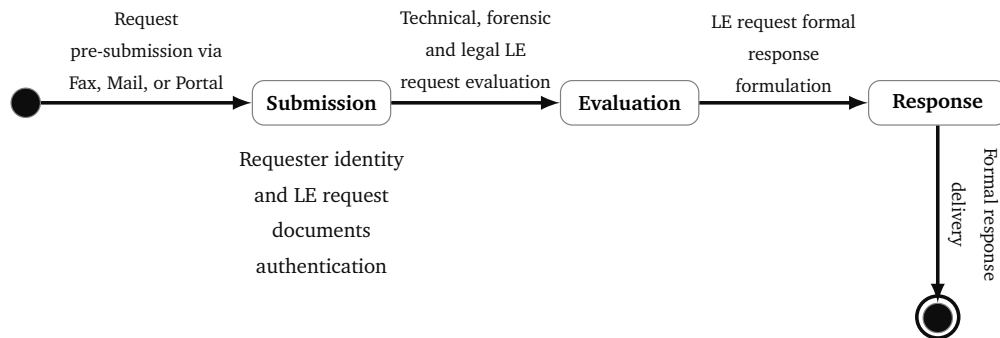


Figure 9.1. LE request processing workflow.

9.2.2 Architecture definition

With the established LE request processing workflow (Figure. 9.1), the information gathered from CSPs transparency reports, LE guidelines analysis (Section. 8.4), and the composition of the evaluation team, we may sketch an abstract architecture for a law enforcement requests management system (see Figure. 9.2), where it's main modules are the following: (1) Online Law Enforcement Management System (OLEMS), (2) Digital Forensic Investigation Capabilities (DFIC), (3) Digital Evidence Management Capabilities (DEMC), and (4) Cases Management Capabilities (CMC).

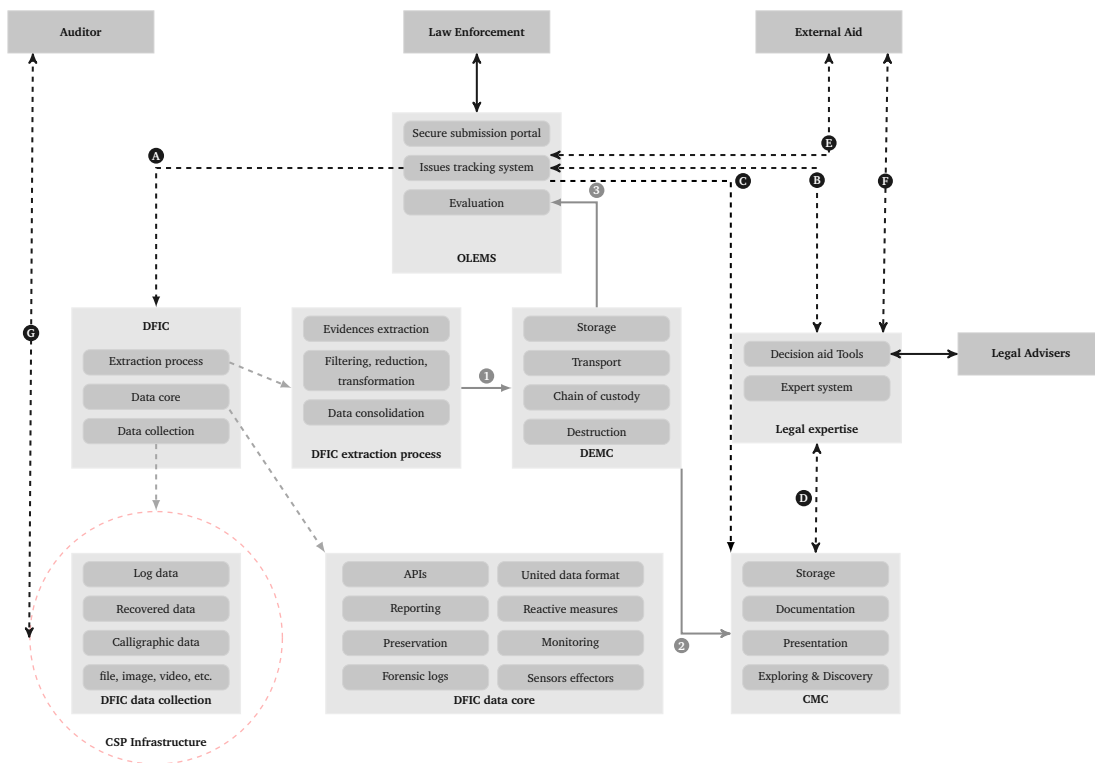


Figure 9.2. An abstract architecture for a law enforcement requests management system.

After the submission phase, if an escalation to a full DFI is required, the Digital Forensic Investigation Capabilities (DFIC) are activated through the (A) connection, and a new case is opened in the Case Management Capability (CMC). Legal expertise may also be solicited through the (B) connection. Once the DFIC is activated, a sound DFI process is engaged. First, the collection of potential digital evidence is made across the CSP's infrastructure using the DFIC *data core* sub-capabilities, then evidence are extracted with the DFIC *extraction process*, and securely managed by the Digital Evidence Management Capabilities (DEMC).

When the required digital evidence are available, they are included in the associated case via the connection (2), and the findings are transmitted to the OLEMS for reporting via the connection (3). Legal advisor's having a secure access to the CMC via the (D) connection may establish their reports based on elements of the current case, and the knowledge that they may have discovered from similar past cases. Once the technical, forensic, and legal reports are available, the CSP formulates a response to the LE, either via the OLEMS or any available legal means.

The next section provides details about the different modules of the proposed architecture.

9.2.2.1 *Online law enforcement management system (OLEMS)*

The goal of this group of capabilities is to improve the interactions between: (1) CSP and LEs, and (2) involved teams in a request processing. It contains the following modules:

1. A secure pre-submission portal to accelerate in some instances the evaluation and response delays. In fact, even if the authenticated documents are required, the emergency and preservation requests may benefit from proactive measures dictated by the evaluation team;
2. An issue tracking system for the internal staff and the LE to monitor the request processing workflow;
3. Productivity tools (information exchange, virtual meeting, redactions tools, etc.) to enhance the collaboration of the involved teams (internal/external).

9.2.2.2 *Digital forensic investigation capabilities (DFIC)*

This group contains the required capabilities that ensure a proper and sound DFI. Inspired by De Marco, M.-T. Kechadi, and Ferrucci, 2014 abstract reference architect, it includes the following modules:

1. Data collection: represents the inventory of the *potential* digital evidence sources and the suited collection tools. Therefore, log data, available and recovered artifacts are gathered among the several layers (physical and virtual) of a CSP' infrastructure from the hardware to the application levels.
2. Data core: regroups the locally and remotely accessible core primitives that are required for evidence collection and analysis, monitoring, data format unification, log preservation, etc.
3. Extraction process: contains the suited tools for data consolidation, filtering, reduction and transformation.

9.2.2.3 *Digital evidences management capabilities (DEMC)*

This group of capabilities aims to ensure evidence safeguard and admissibility, and the preservation of the chain of custody. As shown in Figure. 9.2, this group contains four capabilities: (1) storage, (2) transport, (3) chain of custody and (4) destruction. As for the storage, several formats of digital evidence exist, such as Raw, DEB and AFF4 (Michael Cohen and Schatz, 2010; Prayudi and SN, 2015). In addition to the format, there are also some other attributes related to a storage capability, such as storage area, infrastructure security, and scalability (Cruz, Moser, and Michael Cohen, 2015a). Concerning the transport, in case of a cooperation among several forensic experts, a secure transport capability that ensures the security of digital evidence and the maintenance of the chain of custody is required. Indeed, the preservation of the chain of custody is vital for the admissibility of the collected evidence. Finally, depending on the

associated jurisdiction, destruction of the collected evidence may be considered with the due respect of laws and regulations.

9.2.2.4 Cases management capabilities (CMC)

Usually, when a request is processed, it generates a case that contains elements, such as a digitalized version of the request papers, evaluation reports, briefings notes, artifacts, evidence, and evidence custody documents, etc. CMC capabilities aim to ensure the storage and the preservation of the aforementioned elements. In the next subsection, we provide details on the proposed system requirements.

9.2.3 System requirements

In this section we would like to implement a Proof of Concept (PoC) of the proposed architecture (subsection. 9.2.2). Our methodology is project driven. However, to optimize the costs of the implementation, we have adopted the following guidelines: (1) candidate solutions must be open source, or responder's in-house made, (2) scalability, (3) portability and interoperability. Our implementation should also consider to some other non-functional system requirements, such as (4) Cloud Digital Forensic Readiness (DFR) (*i.e., ability to collect admissible digital evidence while optimising the costs of an investigation*), (5) ensure a transparent LE request handling, and (6) Trust.

Even if the chosen modules are open source, there are still costs related to the Cloud deployment. Nonetheless, in the following sections, we first assess the requirements for each sub-module (Figure. 9.2) in Section. 9.3 and provide an economic assessment of the proposed solutions costs in case of a real world enterprise deployment in Section. 9.6.

9.3 PROTOTYPE DESIGN & DEVELOPMENT

Starting from the OLEMS, a secure LE requests pre-submission portal is required. The request processing may be tracked through a tickets system or any help desk solution. Therefore, there is a need for: Email and SMS notifications; Tickets assignment and management; Dashboards and reporting features. There are many open source solutions that fulfil the cited requirements, such as Osticket, 2020 and Zammad, 2020. In this study, we opted for the osTicket solution as sketched in Figure. 9.3.

In the proposed Proof of Concept (see Figure. 9.3), the connection A, B, C, 1,2 and 3 represent the interactions between sub-modules as specified in the abstract architecture (Section. 9.2.2). However, black coloured box are capabilities that are not implemented in the prototype.

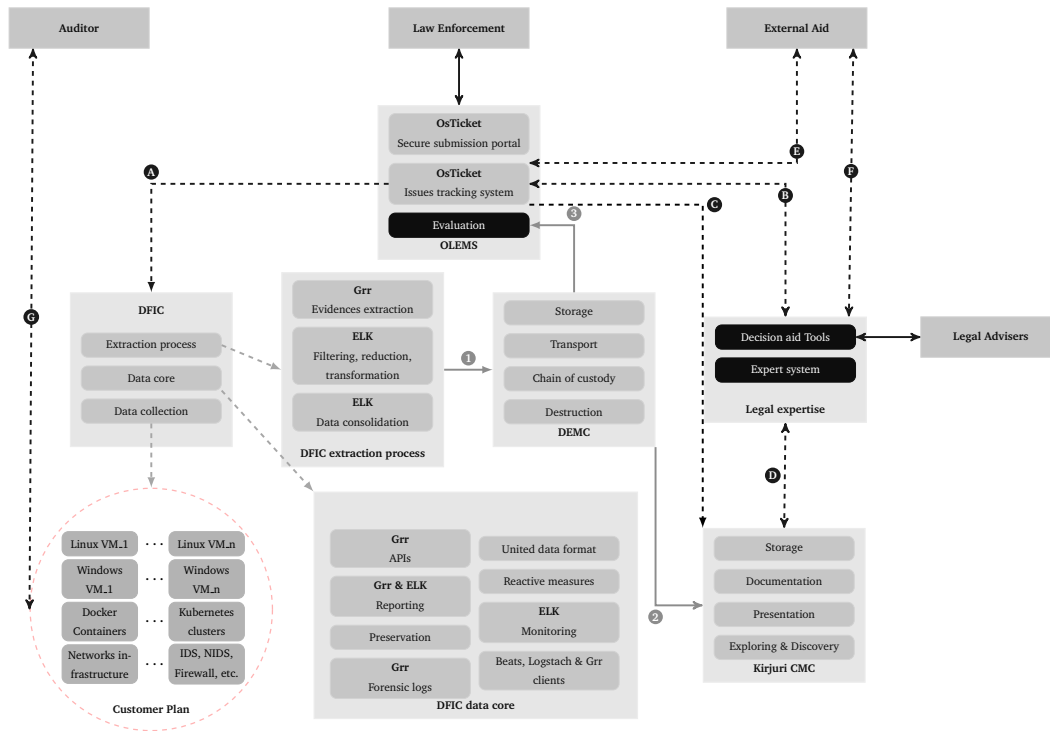


Figure 9.3. A Cloud Law Enforcement Request Management System.

At the reception of the request papers, they are scanned and stored for legal and technical evaluation. So, there is a need for electronic documents management and knowledge discovery solutions.

If a request is approved, an escalation to a full DFI is initiated. Therefore, the use of dedicated tools for live forensic, evidence and log data collection (acquisition), analysis and examination are vital. These tools must support multiple types of artefacts, and ensure secure evidence storage.

For the monitoring and log analysis, we opted for the Elasticsearch Logstash Kibana stack ELK, 2020. Events, network packets and logs are collected via agents (Beats) deployed on the customers plan and forwarded to the Elasticsearch cluster in real-time. The Kibana dashboards help in monitoring, gaining insight, and hunting threats. For the incident response and live forensic, we opted for the Google Rapid Response (Grr) solution (M.I. Cohen, Bilby, and Caronni, 2011; Cruz, Moser, and Michael Cohen, 2015b; Moser and M. I. Cohen, 2013).

Finally, for case management, we opted for the open source solution Kirjuri, 2020 that provides support for: (1) investigators and evidence management, (2) investigation and chain of custody documents (request documents, evaluation reports, evidence analysis reports, etc.) management, digital evidence storage. Note, however, that digital evidence storage and

management may be also done through separated data stores such a MongoDB cluster as suggested in (Cruz, Moser, and Michael Cohen, 2015b).

As for the *evaluation* module and the legal capabilities they are not considered in the developed prototype as they may be ensured by offline (not connected) (in-house made or open source) solutions. Mainly consisting of an assistance and aid tool for reports editing (in case of the evaluation module), and a knowledge database and electronic document discovery for the legal capabilities, those elements may be separated from the connected system.

The following section provides details on the deployment of a proof of concept prototype of the proposed solution on an IaaS infrastructure.

9.4 CLOUD DEPLOYMENT

For the deployment of our prototype, we opted for a Cloud (IaaS) platform (Google, 2020a) as shown in Figure. 9.3. The allocated resources for some modules, such as the Grr-server, Elasticsearch, and Osticket, depend on the customer plan (i.e, number of targeted nodes). In fact, depending on the demand —growth or decrease in the number of client nodes— the deployment of these modules may be scaled up or down.










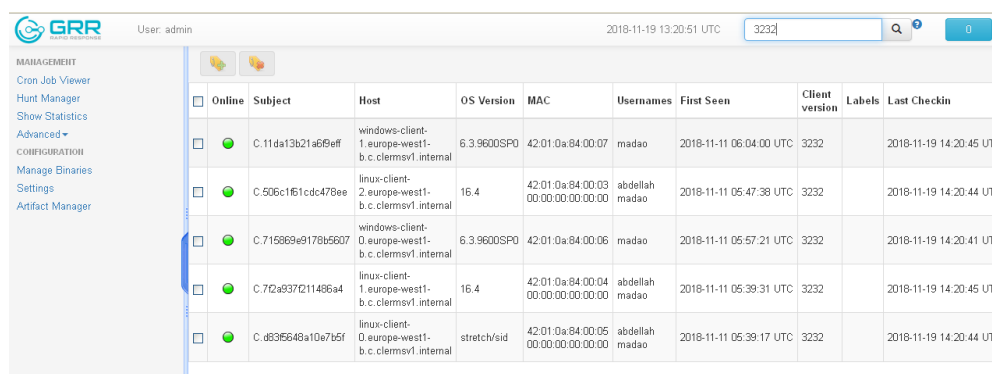
<input type="checkbox"/> Name ^	Zone	Recommendation	Internal IP	External IP	Connect
<input type="checkbox"/>  grr-server	europe-west1-b		10.132.0.2 (nic0)		SSH ▾ ⋮
<input type="checkbox"/>  kirjurivm	europe-north1-a		10.166.0.3 (nic0)		SSH ▾ ⋮
<input type="checkbox"/>  linux-client-0	europe-west1-b		10.132.0.5 (nic0)		SSH ▾ ⋮
<input type="checkbox"/>  linux-client-1	europe-west1-b		10.132.0.4 (nic0)		SSH ▾ ⋮
<input type="checkbox"/>  linux-client-2	europe-west1-b		10.132.0.3 (nic0)		SSH ▾ ⋮
<input type="checkbox"/>  log-monitor-vm	europe-west2-c		10.154.0.2 (nic0)		SSH ▾ ⋮
<input type="checkbox"/>  osticketvm	europe-west4-a		10.164.0.2 (nic0)		SSH ▾ ⋮
<input type="checkbox"/>  windows-client-0	europe-west1-b		10.132.0.6 (nic0)		RDP ▾ ⋮
<input type="checkbox"/>  windows-client-1	europe-west1-b		10.132.0.7 (nic0)		RDP ▾ ⋮

Figure 9.4. CLERMS deployment on an IaaS infrastructure.

In our case, the customer plan contains 5 Virtual Machines (VMs) (3 were Linux based, and two Microsoft Server 2010 instances). For larger deployment, the Grr documents¹ specify the type and requirements for the Grr-server deployment. In our case a single VM instance was enough (see Figure. 9.4); The Grr-server administration interface is shown in Figure. 9.5.

¹ <https://grr-doc.readthedocs.io/en/latest/faq.html>



The screenshot shows the Grr-server administration interface. On the left is a sidebar with navigation links: MANAGEMENT (Cron Job Viewer, Hunt Manager, Show Statistics, Advanced), CONFIGURATION (Manage Binaries, Settings, Artifact Manager), and a search bar. The main area displays a table of agents with columns: Online, Subject, Host, OS Version, MAC, Uname, First Seen, Client version, Labels, and Last Checkin. There are 6 agents listed, all with status 'Online' and client version '3232'.

Online	Subject	Host	OS Version	MAC	Uname	First Seen	Client version	Labels	Last Checkin
<input checked="" type="checkbox"/>	C:11da13b21a6b9eff	windows-client-1.europe-west1-b.c.cloudfoundry.internal	6.3.9600SP0	42:01:0a:84:00:07	madao	2018-11-11 06:04:00 UTC	3232		2018-11-19 14:20:45 UTC
<input checked="" type="checkbox"/>	C:506c1f51cdc478ee	linux-client-2.europe-west1-b.c.cloudfoundry.internal	16.4	42:01:0a:84:00:03	abdellah madao	2018-11-11 05:47:38 UTC	3232		2018-11-19 14:20:44 UTC
<input checked="" type="checkbox"/>	C:715869e9178b5607	windows-client-0.europe-west1-b.c.cloudfoundry.internal	6.3.9600SP0	42:01:0a:84:00:06	madao	2018-11-11 05:57:21 UTC	3232		2018-11-19 14:20:41 UTC
<input checked="" type="checkbox"/>	C:702a937011486a4	linux-client-1.europe-west1-b.c.cloudfoundry.internal	16.4	42:01:0a:84:00:04	abdellah madao	2018-11-11 05:39:31 UTC	3232		2018-11-19 14:20:45 UTC
<input checked="" type="checkbox"/>	C:d83f6648a10e7b5f	linux-client-0.europe-west1-b.c.cloudfoundry.internal	stretch/sid	42:01:0a:84:00:05	abdellah madao	2018-11-11 05:39:17 UTC	3232		2018-11-19 14:20:44 UTC

Figure 9.5. Grr-server administration user interface.

Logging and monitoring are done via agents (LogStach agents, Beats) on the customer's VMs plan. The collected information is forwarded to the ELK cluster. In the production mode—real world case usage—the ELK cluster deployment requires at least three nodes. However, in our case a single node was sufficient. Figure 9.6 shows log visualization through Kibana dashboards.

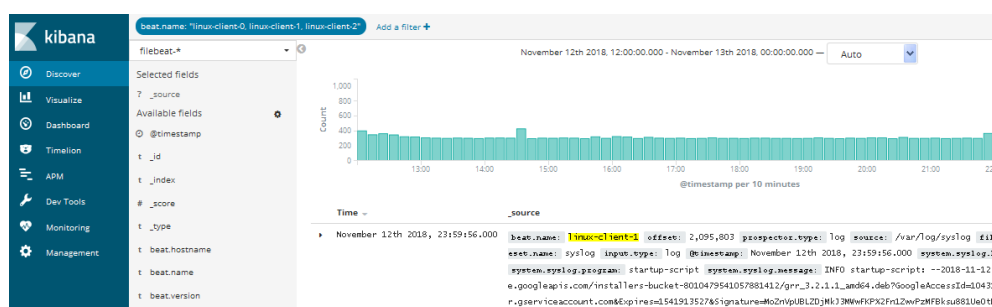


Figure 9.6. Monitoring, logs ingestion, and threat hunting via Kibana dashboards.

The online request pre-submission is done through an osTicket instance (Fig 9.7), which was deployed in a single VM instance. In the case of traffic increase, the scaling up may be achieved through redundancy and load balancing.

The required information for request pre-submission based on LE guidelines (see Section 8.4) are: (a) agent contact information, (b) agent superior contact information, (c) agency contact information, (d) scan of legal documents that support the request, and (e) target information.

When a request is correctly submitted (see Figure 9.7), a notification is sent to the crisis manager. Consultation is then made with the legal assistance, and in some cases an investigation is initiated. In case of escalation, tickets and tasks are forwarded to those concerned by the investigation. At the conclusion of the investigation, elements related to the case are forwarded to the case management solution.

Open a New Ticket
Please fill in the form below to open a new ticket.

Contact Information
Please fill in the contact informations, then proceed to the rest of the required information.

Email Address *

Full Name *

Phone Number Ext *

Help Topic
Law Enforcement *

Law Enforcement Agent Information Contact
Please fill in here all the required information

First Name *

Last Name *

Badge Number *

Email *

Superior Contact Information
Please fill here the required information about your superior

Superior First Name *

Superior Last Name *

Superior Phone Number Ext *

Legal Documents
Please Specify the legal document that support your request

Legal Document Type *

Legal Document Scan Upload *

Law Enforcement Agency Contact
Please give us more information about your agency

Agency Name

Agency Address

Agency contact phone number Ext *

Agency contact email

Target Information
Please specify here information on the Requested target information, you must fill at least one of those input. Please specify whether we can notify the target of ongoing procedure or not. Lookup period.

id

Name

username

email

Notification *

Specify where it is permissible to notify the target of the ongoing investigation, or not.

Actions *

What type of request

Search From *

Search to *

Figure 9.7. Online LE request pre-submission portal

At the reception of the request's documents, a new case is opened in the Kirjuri solution (see Figure. 9.8). The requester and target information, digital evidence, log, briefing, forensic analysis and examination reports are securely stored.

Kirjuri 0.9.2

Front page 2018

Forensic examination requests 2018

Search requests and devices...

No.	Case	Report no.	Crime	Suspect	Investigator	F. exr.	Mob. exr.	Added
1/18	GoogleCC	9999/R:001	Datavahingonteko RL...	alfonso di roya	igor rovenski serge...	Abdellah	-	08.11.2018

Filter by status: No filtering **Now** **Open** **Ready**

Showing a total of 1 devices in 1 requests (0 new, 1 open, 0 ready).

Figure 9.8. Kirjuri open source case management User Interface.

To validate our proposition, two hypothetical cases study are presented in the next section.

9.5 PROTOTYPE VALIDATION

This section provides two hypothetical usage scenarios for the CLERMS framework:(1) user information disclosure request, (2) content removal request.

9.5.0.1 User information disclosure request

A LE agent “Mike Davies” is filling a user content information disclosure request for the target surname “Jhon smith”. The target is suspected of posting illicit content on a discussion forum hosted at <http://www.mydomain.com/fluxbb>. At the request approval, the crisis manager decide to escalate the event to a full DFI. Based on the target associated IP, the investigation team interrogate the customer plan (via the Grr-servers) for more indications. Afterwards, the forensic expert may opt for:

1. Remote raw disk image acquisition for further examining and analysis, or
2. Database files acquisition via the *filefinder* flow (see Grr-server administration panel) on the path “/var/lib/mysql/fluxbb”.

Moreover, when the forensic expert gain the target “Jhon smith” associated registration IP; A comparison with the provided logs from the ELK stack may confirm whether the illicit content was posted from the target IP address or not. Progressively, the associated request case will then contains elements, such as the digital forensic evidence, logs analysis reports, briefing memos, tasks assignment, a clear investigation workflow, and a proper chain of custody documentation. Finally, a response to the request may be provided via the ticket system or by any official mean.

9.5.0.2 User content removal request

The same LE agent is now suspecting that one of the machines in the customer plan is hosting a “Command and Control” program that is in contact with disseminated malware agents. A removal request with a target machine IP address is then formulated. Upon reception of the request, the crisis manager’s main objective is the disinfection of the potential infected machines. A detailed process for such action may be found in M.I. Cohen, Bilby, and Caronni, 2011. However, the forensic expert may also consider the following: (1) analysis of the processes list flow search (see Figure. 9.5) for a potential Command and Control process, (2) proceed to a forensic memory analysis of the suspected machines, and (3) analysis of the logs, SSH transactions, and bash command history, etc. The aforementioned actions may then help to find the identity of the culprit.

These two hypothetical use-cases having validated our proposed CLERMS framework, one could however wonder “how much” would it cost. The next section provides an economic assessment of the CLERMS deployment.

9.6 ECONOMIC ASSESSMENT

The economic optimality of our solution stands on two facts: (1) open source components; therefore there are no related license fees, (2) Cloud based deployment for a pay per usage model and scalability (up or down) on demand. Thus, the CLERMS solution could fit any enterprise or CSPs. Moreover, in the case of compliance to a LE request, the CSP (requested

company) may formulate a concise, detailed, and transparent costs reimbursement invoice based on the deployment costs (hourly/minutes), man power charges, consulting and support fees, etc.

Regarding to the deployment related charges, Table. 9.1 provides an assessment of the CLERMS monthly costs for a customer plan that contains 7000 (7K) nodes which represents the infrastructure of a large enterprise. The costs listed in Table. 9.1 are related to the functioning of the incident response and forensic plan (see Figure. 9.3), to be accurate. Considered as the baseline configuration for both the Grrr and ELK deployment in such a case (a customer plan with 7000 nodes), it may be scaled up and down depending on the usage. Moreover, the responder may opt for additional digital evidence storage capacity such as a mangodb cluster (more than three nodes with additional storage disks) as specified in (Cruz, Moser, and Michael Cohen, 2015a).

Module	Deployment requirements	Monthly costs (\$)
Osticket	1 VM (n1-standard-1) (1 vCPU, 3,75 GB Memory)	24,27
Kirjuri	1 VM (n1-standard-1) (1 vCPU, 3,75 GB Memory)	24,27
ELK	3 VMs (n1-standard-2) (2 vCPU, 7.5 GB Memory), 500 GB Boot disk, 3 persistent disks of 500 GB each Google, 2020b	165,63
Grrr-servers	Recommended Grr, 2020 5 AWS c5a.xlarge (\$0.077 per hour)	1,940.4
	, and one r3.4xlarge Amazon, 2020 (\$1.328 per Hour)	6,693.12
Total		8.847,69

Table 9.1. Economic assessment of CLERMS deployment solution for a customer plane of 7000 nodes.

9.7 OPPORTUNITIES & LIMITS

The proposed solution aims to: (1) ensure a transparent LE request handling, and (2) enable a responder with a due digital forensic readiness capability in order to guarantee the soundness of conducted digital forensic investigation and the admissibility of the collected evidence. Based on open source components it allows : (a) a reduction of inherent in-house or solution acquisition fees, and (b) an effortless integration process. Designed to fit any sized responder (i.e., going for a public CSP to the smallest enterprise that is outsourcing parts of its own IS

to a CSP) the proposed solution will allow a responder to formulate a concise and precise estimation of LE request processing costs reimbursement fees.

By ensuring the due digital forensic readiness, the proposed solution empowers a responder to conduct sound investigations both in case of a response to a legal request, and internally in case of a security incident.

For the legal request processing, the proposed solution induces an automation (and scalability) that for sure will reduce: (1) the request's volume and lower its growth rate, (2) latency and expected response delays.

Distributed and scalable technical solutions are not only considered for a responder. Indeed, it is also recommended for the central entity (OIA) that handles incoming foreign requests via formal channels such as MLAT. Such technical improvements will for sure reduce the case's backlog and processing delays and therefore accelerate the handling of foreign legal requests. In fact, in an effort to reform the MLAT processing, the US Department of Justice has already expressed the following recommendation:

Coordinate with CRM ITM to ensure OIA has access to CRM's Oracle Apex platform and support the automation of OIA's team trackers and leadership dashboards. (USA DOJ, 2021, page 29).

Note that despite these advantages and opportunities, that our framework does not consider in its present form issues, such as multi-tenancy and digital evidence collection in PaaS or SaaS service models.

9.8 SUMMARY

In this chapter, we proposed a Cloud Law Enforcement Requests Management System. Interests in this proposition come from the growth of law enforcement request volume, the latency, and the complexity of requests processing.

Our primary goal was to provide CSPs and organizations with an affordable solution to comply with the received requests. Therefore, we first analysed CSP's transparency reports and law enforcement guidelines. Then, we sketched a request processing workflow, enumerated the involved teams, and provided an abstract architecture. Afterwards, we enumerated the system's requirements, provided a proof of concept prototype based on available open source components, and carried on the deployment phase.

The optimality and validity of our proposition was shown through the response to two hypothetical scenarios and an economic assessment of its related costs. As a future work, we would like to investigate how to integrate automatic (or semi-automatic) request evaluation via decision aid tools and legal expert systems.

Finally, we were concerned by some technical aspects of the proposition, for instance, it may be interesting to investigate in details the associated organizational efforts such the law enforcement policy.

CONCLUSION AND FUTURE WORK

10.1 Conclusion	110
10.2 Future Work	112

10.1 CONCLUSION

Cloud computing is certainly paving the way to the venue of more pervasive technologies than the actual ones. Some ideas that were mere speculations (or *fantasies*) in the past are becoming real. Omni-connectivity and automation backed by limitless and on-demand computing resources are creating a physical reality that is tightly tied to the digital one. The last brick into this new vision is the automation of decision through artificial intelligence, which is also advancing rapidly. While hoping for the best, humans must also prepare for the worst.

Every technological advancement may lead to new opportunities as it may also become a source of new threats and risks. Incidents and crime (or cyber-crime) happen, they are not a matter of *if*, but *when*. When the worst happens, the investigation of its causes is primordial. While digital forensic investigation of these emerging ecosystems may seem complex, ensuring that such a process is *feasible* is even more challenging.

In order to maintain the equilibrium between: (1) technological advancement induced threats, risks and incidents, and (2) security measures, and investigative methods and tools, an advancement in digital forensic science is ultimately required.

Sometimes, evolution requires a shift in perspective — or thinking outside the box —. Even if Forensic-by-Design seems a promising candidate for such an evolution, it may not be. The limits of this new paradigm have been hypothesized and proven for at least a category of open boundaries systems such as Cloud computing backed ones. While our proposition brings some advancements, it still has its limitations.

As a matter of fact, mitigating one challenge at a time may seem like a viable option even when it ignores the inherent non-linear dependency between Cloud forensics issues. In this sense, we made a proposition to mitigate the Multi-jurisdictions issue.

There is still a window of opportunities to maintain a viable gap between the advance of the speculated new *reality*, and how to secure it and investigate it in case of an incident or a “cyber” crime.

One of the slightest opportunities consists in making the different stakeholders (designer, researchers, agencies, states, end-users, etc.) aware of the potential emergence of new risks and threats, and that the likelihood of a digital event (or incident) having an impact on a physical asset is not negligible.

Urging researchers, developers and inventors to integrate the forensics requirements during the design and development of their projects is a first step. Other ones may be achieved by maintaining of the product's (or the system's) forensic-ready state throughout its life cycle.

Along this study, we argued in favour of this vision. As a matter of fact, the first contribution of this thesis demonstrates that while "*Forensic-by-design*" is trending, it is still inefficient in ensuring the due forensic readiness of emergent cloud ecosystems and any open boundaries systems. Upon pointing out the observed weaknesses, we managed to propose an improved *Forensic-by-design* framework with compliance to systems and software engineering standards. The proposed framework is generic, it may be used for any system, and addresses at the same time the observed gaps in the "*Forensic-by-design*" paradigm and position it rightly in the system and software engineering perspective.

In the same line of thought. The second contribution focuses on assessing the opportunities and challenges that may arise from adopting the *Forensic-by-design* strategy in the design and development of "*Forensic-ready*" systems. For this purpose an Intelligent Transportation System was considered. In addition to clearly stating and defining that *Forensic-ready* is a temporal system's state, the second contribution shows that while there are real opportunities in achieving such a goal (Forensic-ready *ITS*), there are still some persistent challenges. Among the factors that may delay the achievement of *Forensic-ready* systems, we may cite the stakeholders' lack of awareness. Indeed, even in the most pervasive systems (*ITS*), the associated stakeholders still focus more on the *physical* aspects of the system rather than the *digital* ones. Ensuring that the involved actors in the design and development of a system are aware of the risks that may cause a security incident or a cyber-crime on physical assets is the first step. In fact, among the activities that are accomplished during the *design* of a system, the "*architecture definition*" activity is crucial. An architecture is the expression of the stakeholders' concerns. Therefore, making stakeholders aware of the requirement for digital evidence in case of security incidents or cyber-crimes is the starting point in the envisioned efforts towards the integration of forensic requirement in the design and development of a system, and finally towards the achievement of a *Forensic-ready* system.

The third contribution takes on another Cloud Forensics major issue which is *multi-jurisdictions*. More precisely, it investigates how to ensure a responder with the due capabilities to respond and manage Law Enforcement requests. Through this contribution, a description of *LE* formal and informal channels for cross-borders data access, an analysis of majors *CSPs* transparency reports and *LE* guidelines, proposition of an architecture for *LE* requests management system, development and deployment of a prototype, and finally validation of the Cloud Law Enforcement Request Management System through some hypothetical scenarios. More importantly, this third contribution confirms the non-linear dependency between *CF* challenges and at the same time exhibits the opportunities that may emerge from using technical capabilities to aid in mitigating legal or organisational issues. Such an approach may help the research to think outside the box when dealing with legal or organisation challenges. As a matter of fact, the *LE* formal channel access to cross-borders data suffers from latency, which is not only due the complexity of the associated legal procedures but also the volume of the request backlog,

adoption a cloud based processing solution may for sure reduce the latency, and therefore accelerate the treatment of [LE](#) requests. The adopted approach in this third contribution may be generalized in resolving other legal or organisational challenges through addressing the adjacent technical issues.

In summary, an important take away from our study is that, similarly to any scientific domain, people, companies, and organisations should not apprehend the adoption of technological evolution—even without a perfect security—, as long as these advancements are also adopted to stimulate new ways for securing and investigating the resulting ecosystems.

10.2 FUTURE WORK

While thinking about the advance of a new reality which is triggered by technological progress is stimulating, anticipating the emergence of new risks and ensuring the preparedness of this new reality to host digital forensic investigation is *vital*. For future work, we are already investigating two axes:

1. Specification of *forensic-ready* systems,
2. Assessment of the opportunities and challenges of digital forensics in artificial intelligence backed systems.

BIBLIOGRAPHY

- Abraha, Halefom H (July 2019). "How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis". In: *International Data Privacy Law* 9.3, pp. 207–215. DOI: [10.1093/idpl/ipz009](https://doi.org/10.1093/idpl/ipz009). URL: <https://doi.org/10.1093/idpl/ipz009>.
- Act, Accountability (1996). "Health insurance portability and accountability act of 1996". In: *Public law* 104, p. 191.
- Alam, Muhammad, Joaquim Ferreira, and José Fonseca (2016). "Introduction to Intelligent Transportation Systems". In: *Intelligent Transportation Systems*. Springer International Publishing, pp. 1–17. DOI: [10.1007/978-3-319-28183-4_1](https://doi.org/10.1007/978-3-319-28183-4_1). URL: https://doi.org/10.1007/978-3-319-28183-4_1.
- Alenezi, Ahmed, Raid Khalid Hussein, Robert J. Walters, and Gary B. Wills (Apr. 2017). "A Framework for Cloud Forensic Readiness in Organizations". In: *2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*. IEEE, pp. 199–204. DOI: [10.1109/mobilecloud.2017.12](https://doi.org/10.1109/mobilecloud.2017.12). URL: <https://doi.org/10.1109/mobilecloud.2017.12>.
- Alex, M. Edington and R. Kishore (2017). "Forensics framework for cloud computing". In: *Computers & Electrical Engineering* 60, pp. 193–205. ISSN: 0045-7906. DOI: <https://doi.org/10.1016/j.compeleceng.2017.02.006>. URL: <https://www.sciencedirect.com/science/article/pii/S0045790617302689>.
- Alliance, Cloud Security (2019). *Cloud Controls Matrix*. Accessed on 27.01.2021. URL: <https://cloudsecurityalliance.org/research/cloud-controls-matrix/>.
- Amazon (2020). *Amazon AWS Pricing*. Accessed: 2020-07-11. URL: <https://aws.amazon.com/ec2/pricing/reserved-instances/pricing> (visited on).
- Amazon (2021). *Amazon Law Enforcement Guidelines*. Accessed: 2021-01-28. URL: https://d1.awsstatic.com/certifications/Amazon%5C_LawEnforcement%5C_Guidelines.pdf (visited on 01/28/2021).
- Awuson-David, Kenny, Tawfik Al-Hadhrani, Mamoun Alazab, Nazaraf Shah, and Andrii Shalaginov (2021). "BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem". In: *Future Generation Computer Systems* 122, pp. 1–13. ISSN: 0167-739X. DOI: <https://doi.org/10.1016/j.future.2021.03.001>. URL: <https://www.sciencedirect.com/science/article/pii/S0167739X21000807>.
- Badger, Lee et al. (Oct. 2014). *US Government Cloud Computing Technology Roadmap*. Tech. rep. National Institute of Standards and Technology. DOI: [10.6028/nist.sp.500-293](https://doi.org/10.6028/nist.sp.500-293). URL: <https://doi.org/10.6028/nist.sp.500-293>.
- Badger, M L, T Grance, R Patt-Corner, and J Voas (2012). *Cloud computing synopsis and recommendations*. Tech. rep. National Institute of Standards and Technology. DOI: [10.6028/nist.sp.800-146](https://doi.org/10.6028/nist.sp.800-146). URL: <https://doi.org/10.6028/nist.sp.800-146>.

- Battistoni, Roberto, Roberto Di Pietro, and Flavio Lombardi (Oct. 2016). "CURE—Towards enforcing a reliable timeline for cloud forensics: Model, architecture, and experiments". In: *Computer Communications* 91-92, pp. 29-43. DOI: [10.1016/j.comcom.2016.03.024](https://doi.org/10.1016/j.comcom.2016.03.024). URL: <https://doi.org/10.1016/j.comcom.2016.03.024>.
- Bilgic, Secil (2018). "Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act". In: *Harv. JL & Tech.* 32, p. 321.
- Bollé, Timothy, Eoghan Casey, and Maëlig Jacquet (Sept. 2020). "The role of evaluations in reaching decisions using automated systems supporting forensic analysis". In: *Forensic Science International: Digital Investigation* 34, p. 301016. DOI: [10.1016/j.fsidi.2020.301016](https://doi.org/10.1016/j.fsidi.2020.301016). URL: <https://doi.org/10.1016/j.fsidi.2020.301016>.
- Buyya, Rajkumar, Chee Shin Yeo, and Srikumar Venugopal (Sept. 2008). "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities". In: *2008 10th IEEE International Conference on High Performance Computing and Communications*. IEEE. DOI: [10.1109/hpcc.2008.172](https://doi.org/10.1109/hpcc.2008.172). URL: <https://doi.org/10.1109/hpcc.2008.172>.
- Canada, Transport (2021). *ITS Architecture for Canada*. Accessed: 2021-06-08. URL: <https://www.itscanada.ca/about/architecture/index.html> (visited on).
- Carrier, Brian and Eugene Spafford (2004). "An event-based digital forensic investigation framework". In: *Digital Investigation*.
- Casey, Eoghan (2011). *Digital Evidence and Computer Crime Forensic Science and Computers and the Internet*. Third Edition. ISBN 978-0-12-374268-1. Elsevier.
- Cavoukian, Ann (2012). "Privacy by Design [Leading Edge]". In: *IEEE Technology and Society Magazine* 31.4, pp. 18-19. DOI: [10.1109/mts.2012.2225459](https://doi.org/10.1109/mts.2012.2225459). URL: <https://doi.org/10.1109/mts.2012.2225459>.
- Chan-Edmiston, Sharon, Stephanie Fischer, Suzanne Sloan, and Melissa Wong (2020). *Intelligent Transportation Systems (ITS) Joint Program Office: Strategic Plan 2020-2025*. Tech. rep. U.S. Department of Transportation. URL: https://www.its.dot.gov/stratplan2020/ITSJPO%5C_StrategicPlan%5C_2020-2025.pdf.
- Choo, Kim-Kwang Raymond (2014). "Legal Issues in the Cloud". In: *IEEE Cloud Computing* 1.1, pp. 94-96. DOI: [10.1109/MCC.2014.14](https://doi.org/10.1109/MCC.2014.14).
- Choo, Kim-Kwang Raymond, Christian Esposito, and Aniello Castiglione (2017). "Evidence and forensics in the cloud: Challenges and future research directions". In: *IEEE Cloud Computing* 4.3, pp. 14-19.
- Choo, Kim-Kwang Raymond, Martin Herman, Michaela Iorga, and Ben Martini (Sept. 2016). "Cloud forensics: State-of-the-art and future directions". In: *Digital Investigation* 18, pp. 77-78. DOI: [10.1016/j.diin.2016.08.003](https://doi.org/10.1016/j.diin.2016.08.003). URL: <https://doi.org/10.1016/j.diin.2016.08.003>.
- Ciardhuáinand, Séamus Ó (2004). "An extended model of cybercrime investigations". In: *International Journal of Digital Evidence* 3.1, pp. 1-22.
- Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone (Aug. 2012). *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*.

- Tech. rep. National Institute of Standards and Technology. DOI: [10.6028/nist.sp.800-61r2](https://doi.org/10.6028/nist.sp.800-61r2). URL: <https://doi.org/10.6028/nist.sp.800-61r2>.
- Cohen, Aviad and Nir Nissim (2018). "Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory". In: *Expert Systems with Applications* 102, pp. 158–178. ISSN: 0957-4174. DOI: <https://doi.org/10.1016/j.eswa.2018.02.039>. URL: <https://www.sciencedirect.com/science/article/pii/S0957417418301283>.
- Cohen, M.I., D. Bilby, and G. Caronni (Aug. 2011). "Distributed forensics and incident response in the enterprise". In: *Digital Investigation* 8, S101–S110. DOI: [10.1016/j.diin.2011.05.012](https://doi.org/10.1016/j.diin.2011.05.012). URL: <https://doi.org/10.1016/j.diin.2011.05.012>.
- Cohen, Michael and Bradley Schatz (Aug. 2010). "Hash based disk imaging using AFF4". In: *Digital Investigation* 7, S121–S128. DOI: [10.1016/j.diin.2010.05.015](https://doi.org/10.1016/j.diin.2010.05.015). URL: <https://doi.org/10.1016/j.diin.2010.05.015>.
- Colman-Meixner, Carlos, Chris Develder, Massimo Tornatore, and Biswanath Mukherjee (2016). "A Survey on Resiliency Techniques in Cloud Computing Infrastructures and Applications". In: *IEEE Communications Surveys & Tutorials* 18.3, pp. 2244–2281. DOI: [10.1109/comst.2016.2531104](https://doi.org/10.1109/comst.2016.2531104). URL: <https://doi.org/10.1109/comst.2016.2531104>.
- Cruz, Flavio, Andreas Moser, and Michael Cohen (Mar. 2015a). "A scalable file based data store for forensic analysis". In: *Digital Investigation* 12, S90–S101. DOI: [10.1016/j.diin.2015.01.016](https://doi.org/10.1016/j.diin.2015.01.016). URL: <https://doi.org/10.1016/j.diin.2015.01.016>.
- Cruz, Flavio, Andreas Moser, and Michael Cohen (Mar. 2015b). "A scalable file based data store for forensic analysis". In: *Digital Investigation* 12, S90–S101. DOI: [10.1016/j.diin.2015.01.016](https://doi.org/10.1016/j.diin.2015.01.016). URL: <https://doi.org/10.1016/j.diin.2015.01.016>.
- Daskal, Jennifer (2018). "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0". In: *Stan. L. Rev. Online* 71, p. 9.
- De La Torre, Gonzalo, Paul Rad, and Kim-Kwang Raymond Choo (July 2020). "Driverless vehicle security: Challenges and future research opportunities". In: *Future Generation Computer Systems* 108, pp. 1092–1111. DOI: [10.1016/j.future.2017.12.041](https://doi.org/10.1016/j.future.2017.12.041). URL: <https://doi.org/10.1016/j.future.2017.12.041>.
- De Marco, Lucia, M-Tahar Kechadi, and Filomena Ferrucci (2014). "Cloud Forensic Readiness: Foundations". In: *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Springer International Publishing, pp. 237–244. DOI: [10.1007/978-3-319-14289-0_16](https://doi.org/10.1007/978-3-319-14289-0_16). URL: https://doi.org/10.1007/978-3-319-14289-0_16.
- Dilijonaite, Ausra (May 2017). "Digital Forensic Readiness". In: *Digital Forensics*. John Wiley & Sons, Ltd, pp. 117–145. DOI: [10.1002/9781119262442.ch4](https://doi.org/10.1002/9781119262442.ch4). URL: <https://doi.org/10.1002/9781119262442.ch4>.
- DMTF, Open (2015). *Virtualization Format Specification Version 1.0.0*. URL: https://www.dmtf.org/sites/default/files/standards/documents/DSP0243_2.1.1.pdf.
- DOJ, U.S.A (2018). *Clarifying Lawful Overseas Use of Data (CLOUD) Act*. Accessed: 2020-07-11. URL: <https://www.justice.gov/dag/page/file/1236281/download>.

- DOJ, U.S.A (2020). *Cloud act ressources*. Accessed: 2020-07-11. URL: <https://www.justice.gov/dag/cloudact> (visited on).
- DOJ, USA (2014). *U.S. Department of Justice FY 2015 Budget*. URL: <http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf>.
- DOJ, USA (2021). *Audit of the Criminal Division's Process for Incoming Mutual Legal Assistance Requests Audit Division*. URL: <https://oig.justice.gov/sites/default/files/reports/21-097.pdf>.
- DoT, U.S. (2021a). *ARC-IT life cycle*. Accessed: 2021-06-08. URL: <https://local.iteris.com/arc-it/html/viewpoints/systemlifecycle.html> (visited on).
- DoT, U.S. (2021b). *ARC-IT Organizational controls*. Accessed: 2021-06-08. URL: <https://local.iteris.com/arc-it/html/security/organizationalcontrols.html> (visited on).
- DoT, U.S. (2021c). *ARC-IT Resiliency*. Accessed: 2021-06-08. URL: <https://local.iteris.com/arc-it/html/archuse/goal9.html> (visited on).
- DoT, U.S. (2021d). *ARC-IT Security*. Accessed: 2021-06-08. URL: <https://local.iteris.com/arc-it/html/security/security.html> (visited on).
- DoT, U.S. (2021e). *Architecture Reference for Cooperative and Intelligent Transportation*. Accessed: 2021-06-08. URL: <https://local.iteris.com/arc-it/> (visited on).
- ELK (2020). *ElasticSearch*. Accessed: 2020-07-11. URL: <https://www.elastic.co> (visited on).
- Endicott-Popovsky, Barbara, Deborah A. Frincke, and Carol A. Taylor (May 2007). "A Theoretical Framework for Organizational Network Forensic Readiness". In: *Journal of Computers* 2.3, pp. 1–11. DOI: [10.4304/jcp.2.3.1-11](https://doi.org/10.4304/jcp.2.3.1-11). URL: <https://doi.org/10.4304/jcp.2.3.1-11>.
- ETSI (2021). *ITS Europe*. Accessed: 2021-06-08. URL: <https://www.etsi.org/technologies/automotive-intelligent-transport> (visited on).
- Facebook (2020a). *Company Information*. Accessed: 2020-07-11. URL: <https://about.fb.com/company-info/> (visited on).
- Facebook (2020b). *Facebook Law Enforcement Guidelines*. Accessed: 2020-07-11. URL: <https://www.facebook.com/safety/groups/law/guidelines/> (visited on 07/11/2020).
- Facebook (2020c). *Law Enforcement Online Requests*. Accessed: 2020-07-11. URL: <https://www.facebook.com/records/login/> (visited on 07/11/2020).
- Faheem, Muhammad, M. Tahar Kechadi, and Nhien-An Le-Khac (2015). "The State of the Art Forensic Techniques in Mobile Cloud Environment: A Survey, Challenges and Current Trends". In: *Int. J. Digit. Crime Forensics* 7.2, pp. 1–19. DOI: [10.4018/ijdcf.2015040101](https://doi.org/10.4018/ijdcf.2015040101). URL: <https://doi.org/10.4018/ijdcf.2015040101>.
- Team, National ITS Architecture (2007a). *System Engineering for Intelligent Transportation Systems*. Technical Report. 1515 S. Manchester Ave. Anaheim, CA 92802. USA: Iteris, Inc. URL: <https://ops.fhwa.dot.gov/publications/seitsguide/>.
- Team, National ITS Architecture (2007b). *System Engineering for Intelligent Transportation Systems*. Technical Report. 1515 S. Manchester Ave. Anaheim, CA 92802. USA: Iteris, Inc.
- Figueiredo, L., I. Jesus, J.A.T. Machado, J.R. Ferreira, and J.L. Martins de Carvalho (2001). "Towards the development of intelligent transportation systems". In: *ITSC 2001. 2001 IEEE*

- Intelligent Transportation Systems. Proceedings (Cat. No.01TH8585)*. IEEE. DOI: [10.1109/itsc.2001.948835](https://doi.org/10.1109/itsc.2001.948835). URL: <https://doi.org/10.1109/itsc.2001.948835>.
- Fondation, Electronic Frontier (2015). *Warrant for Microsoft Email Stored in Dublin, Ireland*. URL: <https://www.eff.org/fr/cases/re-warrant-microsoft-email-stored-dublin-ireland>.
- Funk, T. Markus (2014). "Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges". In: *Stanford Public Law Working Paper*.
- Ganin, Alexander A., Avi C. Mersky, Andrew S. Jin, Maksim Kitsak, Jeffrey M. Keisler, and Igor Linkov (Mar. 2019). "Resilience in Intelligent Transportation Systems (ITS)". In: *Transportation Research Part C: Emerging Technologies* 100, pp. 318–329. DOI: [10.1016/j.trc.2019.01.014](https://doi.org/10.1016/j.trc.2019.01.014). URL: <https://doi.org/10.1016/j.trc.2019.01.014>.
- Gartner (2019). *Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019*. Accessed on 27.01.2021. URL: <https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g>.
- Google (2017). *Digital Security and Due Process: Modernizing Cross-Border Surveillance Law for the Cloud Era*. Accessed: 2020-07-11. URL: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/CrossBorderLawEnforcementRequestsWhitePaper%5C_2.pdf (visited on 07/11/2020).
- Google (2020a). *Google Cloud*. Accessed: 2020-07-11. URL: <https://cloud.google.com> (visited on).
- Google (2020b). *Google Cloud ElasticSearch deployment*. Accessed: 2020-07-11. URL: <https://console.cloud.google.com/marketplace/details/click-to-deploy-images/elasticsearch> (visited on).
- Google (2020c). *Google data centre locations*. Accessed: 2020-07-11. URL: <https://www.google.com/about/datacenters/inside/locations/> (visited on).
- Google (2020d). *Google Legal Process*. Accessed: 2020-07-11. URL: <https://support.google.com/transparencyreport/answer/9713961?hl=en> (visited on 07/11/2020).
- Google (2020e). *Law Enforcement Request System*. Accessed: 2020-07-11. URL: https://lers.google.com/signup%5C_v2/landing?hl=en (visited on 07/11/2020).
- Goudbeek, Arnoud, Kim-Kwang Raymond Choo, and Nhien-An Le-Khac (Aug. 2018). "A Forensic Investigation Framework for Smart Home Environment". In: *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE. DOI: [10.1109/trustcom/bigdatase.2018.00201](https://doi.org/10.1109/trustcom/bigdatase.2018.00201). URL: <https://doi.org/10.1109/trustcom/bigdatase.2018.00201>.
- Grispos, George, Jesus Garcia-Galan, Liliana Pasquale, and Bashar Nuseibeh (May 2017). "Are you ready? Towards the engineering of forensic-ready systems". In: *2017 11th International Conference on Research Challenges in Information Science (RCIS)*. IEEE. DOI: [10.1109/rcis.2017.7956555](https://doi.org/10.1109/rcis.2017.7956555). URL: <https://doi.org/10.1109/rcis.2017.7956555>.
- Grispos, George, William Bradley Glisson, and Kim-Kwang Raymond Choo (July 2017). "Medical Cyber-Physical Systems Development: A Forensics-Driven Approach". In: *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies*

- (CHASE). IEEE. DOI: [10.1109/chase.2017.68](https://doi.org/10.1109/chase.2017.68). URL: <https://doi.org/10.1109/chase.2017.68>.
- Grispos, George, Tim Storer, and William Bradley Glisson (2012). "Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics". In: *Int. J. Digit. Crime Forensics* 4.2, pp. 28–48. DOI: [10.4018/jdcf.2012040103](https://doi.org/10.4018/jdcf.2012040103). URL: <https://doi.org/10.4018/jdcf.2012040103>.
- Grr, Google (2020). *Google Grr FAQ*. Accessed: 2020-07-11. URL: <https://grr-doc.readthedocs.io/en/latest/faq.html> (visited on).
- Haley, C.B., R. Laney, J.D. Moffett, and B. Nuseibeh (Jan. 2008). "Security Requirements Engineering: A Framework for Representation and Analysis". In: *IEEE Transactions on Software Engineering* 34.1, pp. 133–153. DOI: [10.1109/tse.2007.70754](https://doi.org/10.1109/tse.2007.70754). URL: <https://doi.org/10.1109/tse.2007.70754>.
- Herman, Martin et al. (Aug. 2020). *NIST cloud computing forensic science challenges*. Tech. rep. National Institute of Standards and Technology. DOI: [10.6028/nist.ir.8006](https://doi.org/10.6028/nist.ir.8006). URL: <https://doi.org/10.6028/nist.ir.8006>.
- Holt, Thomas and Diana S. Dolliver (June 2021). "Exploring digital evidence recognition among front-line law enforcement officers at fatal crash scenes". In: *Forensic Science International: Digital Investigation* 37, p. 301167. DOI: [10.1016/j.fsidi.2021.301167](https://doi.org/10.1016/j.fsidi.2021.301167). URL: <https://doi.org/10.1016/j.fsidi.2021.301167>.
- Huq, Numaan, Rainer Vosseler, and Morton Swimmer (2017). "Cyberattacks against intelligent transportation systems". In: *TrendLabs Research Paper*.
- Initiative, Joint Task Force Transformation (Dec. 2018). *Risk management framework for information systems and organizations*: tech. rep. National Institute of Standards and Technology. DOI: [10.6028/nist.sp.800-37r2](https://doi.org/10.6028/nist.sp.800-37r2). URL: <https://doi.org/10.6028/nist.sp.800-37r2>.
- Inquirer, The Philadelphia (2021). *SEPTA was attacked by ransomware, sources say. It's still restoring operations stifled since August*. Accessed: 2021-06-08. URL: <https://www.inquirer.com/transportation/septa-malware-attack-ransomware-fbi-employees-cybersecurity-20201007.html> (visited on).
- Insights, Fortune Business (2021). *Intelligent Transportation System Market Size, Share and Global Industry Trend Forecast till 2025*. Accessed: 2021-06-08. URL: <https://www.fortunebusinessinsights.com/enquiry/request-sample-pdf/intelligent-transportation-system-market-102065> (visited on).
- Irfan, Muhammad, Haider Abbas, Yunchuan Sun, Anam Sajid, and Maruf Pasha (July 2016). "A framework for cloud forensics evidence collection and analysis using security information and event management". In: *Security and Communication Networks* 9.16, pp. 3790–3807. DOI: [10.1002/sec.1538](https://doi.org/10.1002/sec.1538). URL: <https://doi.org/10.1002/sec.1538>.
- Systems and software engineering — Software life cycle processes* (Nov. 2017). Standard. Geneva, CH: International Organization for Standardization. URL: <https://www.iso.org/standard/43447.html>.

- Systems and software engineering — System life cycle processes* (May 2015). Standard. Geneva, CH: International Organization for Standardization. URL: <https://www.iso.org/standard/63711.html>.
- Systems and software engineering — Life cycle processes — Risk management* (Dec. 2006). Standard. Geneva, CH: International Organization for Standardization. URL: <https://www.iso.org/standard/40723.html>.
- Information technology — Cloud computing — Reference architecture* (2014). Standard. Geneva, CH: International Organization for Standardization. URL: <https://www.iso.org/standard/60545.html>.
- Systems and software engineering — Life cycle management — Part1: Guidelines for life cycle management* (Nov. 2018). Standard. Geneva, CH: International Organization for Standardization. URL: <https://www.iso.org/standard/72896.html>.
- Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management* (Nov. 2016). Standard. Geneva, CH: International Organization for Standardization. URL: <https://www.iso.org/standard/60803.html>.
- Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response* (Nov. 2016). Standard. Geneva, CH: International Organization for Standardization. URL: <https://www.iso.org/standard/62071.html>.
- Information technology — Security techniques — Incident investigation principles and processes* (2015). Standard. Geneva, CH: International Organization for Standardization. URL: <https://www.iso.org/standard/44407.html>.
- Information technology — Security techniques – Privacy framework* (Dec. 2011). Standard. Geneva, CH: International Organization for Standardization. URL: <https://www.iso.org/standard/45123.html>.
- Systems and software engineering — Architecture description* (2015). Standard. Geneva, CH: International Organization for Standardization. URL: <https://www.iso.org/standard/50508.html>.
- Information technology — Security techniques — Privacy engineering for system life cycle processes* (Sept. 2019). Standard. Geneva, CH: International Organization for Standardization. URL: <https://www.iso.org/standard/72024.html>.
- Systems and software engineering — Life cycle processes – Requirements engineering* (Sept. 2018). Standard. Geneva, CH: International Organization for Standardization. URL: <https://www.iso.org/standard/72089.html>.
- James, Joshua I. and Pavel Gladyshev (Sept. 2016). "A survey of mutual legal assistance involving digital evidence". In: *Digital Investigation* 18, pp. 23–32. DOI: [10.1016/j.diin.2016.06.004](https://doi.org/10.1016/j.diin.2016.06.004). URL: <https://doi.org/10.1016/j.diin.2016.06.004>.
- Karagiannis, Christos and Kostas Vergidis (2021). "Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal". In: *Inf.* 12.5, p. 181. DOI: [10.3390/info12050181](https://doi.org/10.3390/info12050181). URL: <https://doi.org/10.3390/info12050181>.
- Kebande, Victor R., Stacey O. Baror, Reza M. Parizi, Kim-Kwang Raymond Choo, and H.S. Venter (Dec. 2020). "Mapping digital forensic application requirement specification to an

- international standard". In: *Forensic Science International: Reports* 2, p. 100137. DOI: [10.1016/j.fsir.2020.100137](https://doi.org/10.1016/j.fsir.2020.100137). URL: <https://doi.org/10.1016/j.fsir.2020.100137>.
- Kebande, Victor R. and H. S. Venter (Jan. 2017). "Novel digital forensic readiness technique in the cloud environment". In: *Australian Journal of Forensic Sciences* 50.5, pp. 552–591. DOI: [10.1080/00450618.2016.1267797](https://doi.org/10.1080/00450618.2016.1267797). URL: <https://doi.org/10.1080/00450618.2016.1267797>.
- Kebande, Victor R. and H.S. Venter (Aug. 2015). "Adding event reconstruction to a Cloud Forensic Readiness model". In: *2015 Information Security for South Africa (ISSA)*. IEEE, pp. 1–9. DOI: [10.1109/issa.2015.7335050](https://doi.org/10.1109/issa.2015.7335050). URL: <https://doi.org/10.1109/issa.2015.7335050>.
- Kelarestaghi, Kaveh Bakhsh, Kevin Heaslip, Majid Khalilikhah, Antonio Fuentes, and Volker Fessmann (June 2018). "Intelligent Transportation System Security: Hacked Message Signs". In: *SAE International Journal of Transportation Cybersecurity and Privacy* 1.2, pp. 75–90. DOI: [10.4271/11-01-02-0004](https://doi.org/10.4271/11-01-02-0004). URL: <https://doi.org/10.4271/11-01-02-0004>.
- Kent, K, S Chevalier, T Grance, and H Dang (2006). *Guide to integrating forensic techniques into incident response*. Tech. rep. DOI: [10.6028/nist.sp.800-86](https://doi.org/10.6028/nist.sp.800-86). URL: <https://doi.org/10.6028/nist.sp.800-86>.
- Le-Khac, Nhien-An, Daniel Jacobs, John Nijhoff, Karsten Bertens, and Kim-Kwang Raymond Choo (Aug. 2020). "Smart vehicle forensics: Challenges and case study". In: *Future Generation Computer Systems* 109, pp. 500–510. DOI: [10.1016/j.future.2018.05.081](https://doi.org/10.1016/j.future.2018.05.081). URL: <https://doi.org/10.1016/j.future.2018.05.081>.
- Kirjuri (2020). *Kirjuri*. Accessed: 2020-07-11. URL: <https://github.com/AnttiKurittu/kirjuri> (visited on).
- Koops, Bert-Jaap and Morag Goodwin (2014). "Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law". In: *SSRN Electronic Journal*. DOI: [10.2139/ssrn.2698263](https://doi.org/10.2139/ssrn.2698263). URL: <https://doi.org/10.2139/ssrn.2698263>.
- Kopencova, Dagmar and Roman Rak (Oct. 2020). "Issues of Vehicle Digital Forensics". In: *2020 XII International Science-Technical Conference AUTOMOTIVE SAFETY*. IEEE. DOI: [10.1109/automotivesafety47494.2020.9293516](https://doi.org/10.1109/automotivesafety47494.2020.9293516). URL: <https://doi.org/10.1109/automotivesafety47494.2020.9293516>.
- Lallie, Harjinder Singh (2012). "Challenges in applying the ACPO principles in cloud forensic investigations". In: *J. Digit. Forensics Secur. Law* 7.1, pp. 71–86. DOI: [10.15394/jdfsl.2012.1113](https://doi.org/10.15394/jdfsl.2012.1113). URL: <https://doi.org/10.15394/jdfsl.2012.1113>.
- Lamssaggad, Ayyoub, Nabil Benamar, Abdelhakim Senhaji Hafid, and Mounira Msahli (2021). "A Survey on the Current Security Landscape of Intelligent Transportation Systems". In: *IEEE Access* 9, pp. 9180–9208. DOI: [10.1109/access.2021.3050038](https://doi.org/10.1109/access.2021.3050038). URL: <https://doi.org/10.1109/access.2021.3050038>.
- Lin, Tiffany and Mailyn Fidler (2017). "Cross-Border Data Access Reform: A Primer on the Proposed US-UK Agreement". In: *Berkman Klein Center Research Publication* 2017-7.
- Liu, Fang, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger, and Dawn Leaf (2011). *NIST cloud computing reference architecture*. Tech. rep. National Institute of Standards and Technology. DOI: [10.6028/nist.sp.500-292](https://doi.org/10.6028/nist.sp.500-292). URL: <https://doi.org/10.6028/nist.sp.500-292>.

- Lopez, Erik Miranda, Seo Yeon Moon, and Jong Hyuk Park (2016). "Scenario-Based Digital Forensics Challenges in Cloud Computing". In: *Symmetry* 8.10, p. 107. DOI: [10.3390/sym8100107](https://doi.org/10.3390/sym8100107). URL: <https://doi.org/10.3390/sym8100107>.
- Lyod (2017). *Counting the costs*. Accessed on 27.01.2021. URL: <https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost>.
- Lyod (2018). *Cloud Down*. Accessed on 27.01.2021. URL: <https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/cloud-down>.
- Malamas, Vaggelis, Thomas Dasaklis, Panayiotis Kotzanikolaou, Mike Burmester, and Sokratis Katsikas (July 2019). "A Forensics-by-Design Management Framework for Medical Devices Based on Blockchain". In: *2019 IEEE World Congress on Services (SERVICES)*. IEEE. DOI: [10.1109/services.2019.00021](https://doi.org/10.1109/services.2019.00021). URL: <https://doi.org/10.1109/services.2019.00021>.
- Manral, Bharat, Gaurav Somani, Kim-Kwang Raymond Choo, Mauro Conti, and Manoj Singh Gaur (Jan. 2020). "A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions". In: *ACM Computing Surveys (CSUR)* 52.6, pp. 1–38. DOI: [10.1145/3361216](https://doi.org/10.1145/3361216). URL: <https://doi.org/10.1145/3361216>.
- Mell, P M and T Grance (2011). *The NIST definition of cloud computing*. Tech. rep. National Institute of Standards and Technology. DOI: [10.6028/nist.sp.800-145](https://doi.org/10.6028/nist.sp.800-145). URL: <https://doi.org/10.6028/nist.sp.800-145>.
- Meneguette, Rodolfo I., Robson E. De Grande, and Antonio A. F. Loureiro (2018). "Intelligent Transportation Systems". In: *Urban Computing*. Springer International Publishing, pp. 1–21. DOI: [10.1007/978-3-319-93332-0_1](https://doi.org/10.1007/978-3-319-93332-0_1). URL: https://doi.org/10.1007/978-3-319-93332-0_1.
- Microsoft (2020a). *Data Law*. Accessed: 2020-07-11. URL: <https://blogs.microsoft.com/datalaw/our-practices/> (visited on 07/11/2020).
- Microsoft (2020b). *Microsoft Transparency Reports*. Accessed: 2020-07-11. URL: <https://www.microsoft.com/en-us/about/corporate-responsibility/lerr> (visited on 07/11/2020).
- Miller, Charlie (Dec. 2019). "Lessons learned from hacking a car". In: *IEEE Design & Test* 36.6, pp. 7–9. DOI: [10.1109/mdat.2018.2863106](https://doi.org/10.1109/mdat.2018.2863106). URL: <https://doi.org/10.1109/mdat.2018.2863106>.
- Moser, Andreas and Michael I. Cohen (Sept. 2013). "Hunting in the enterprise: Forensic triage and incident response". In: *Digital Investigation* 10.2, pp. 89–98. DOI: [10.1016/j.diin.2013.03.003](https://doi.org/10.1016/j.diin.2013.03.003). URL: <https://doi.org/10.1016/j.diin.2013.03.003>.
- Mulligan, Stephen P (2018). *Cross-Border Data Sharing Under the CLOUD Act*. Congressional Research Service.
- NIST (Dec. 2018). *NIST Risk Management Framework for Information Systems and Organizations*. Tech. rep. National Institute of Standards and Technology. DOI: [10.6028/nist.cswp.01162020](https://doi.org/10.6028/nist.cswp.01162020). URL: <https://doi.org/10.6028/nist.cswp.01162020>.
- NIST (Jan. 2020). *NIST PRIVACY FRAMEWORK: A tool for improving privacy through enterprise risk management*. Tech. rep. National Institute of Standards and Technology. DOI: [10.6028/nist.cswp.01162020](https://doi.org/10.6028/nist.cswp.01162020). URL: <https://doi.org/10.6028/nist.cswp.01162020>.

- Norton (2019). *2019 Data Breaches: 4 Billion Records Breached So Far*. Accessed on 27.01.2021. URL: <https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html>.
- Nypost (2021). *New York Post*. Accessed: 2022-05-09. URL: <https://nypost.com/2021/12/13/mta-timekeeping-system-goes-dark-after-ransomware-attack/> (visited on).
- Olariu, Stephan, Tihomir Hristov, and Gongjun Yan (Mar. 2013). "The Next Paradigm Shift: From Vehicular Networks to Vehicular Clouds". In: *Mobile Ad Hoc Networking*. John Wiley & Sons, Inc., pp. 645–700. DOI: [10.1002/9781118511305.ch19](https://doi.org/10.1002/9781118511305.ch19). URL: <https://doi.org/10.1002/9781118511305.ch19>.
- Omeleze, Stacey and Hein S. Venter (Oct. 2017). "Digital forensic application requirements specification process". In: *Australian Journal of Forensic Sciences* 51.4, pp. 371–394. DOI: [10.1080/00450618.2017.1374456](https://doi.org/10.1080/00450618.2017.1374456). URL: <https://doi.org/10.1080/00450618.2017.1374456>.
- Osticket (2020). *Support Ticketing System*. Accessed: 2020-07-11. URL: <https://www.osticket.com> (visited on).
- Palmer, Gary et al. (2001). "A road map for digital forensic research". In: *First Digital Forensic Research Workshop, Utica, New York*, pp. 27–30.
- Parker, Donn B and DB Parker (1976). *Crime by computer*. Scribner New York.
- Parra, Gonzalo De La Torre, Paul Rad, and Kim-Kwang Raymond Choo (June 2019). "Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities". In: *Journal of Network and Computer Applications* 135, pp. 32–46. DOI: [10.1016/j.jnca.2019.02.022](https://doi.org/10.1016/j.jnca.2019.02.022). URL: <https://doi.org/10.1016/j.jnca.2019.02.022>.
- Pasquale, Liliana, Dalal Alrajeh, Claudia Peersman, Thein Tun, Bashar Nuseibeh, and Awais Rashid (2018). "Towards forensic-ready software systems". In: *Proceedings of the 40th International Conference on Software Engineering New Ideas and Emerging Results - ICSE-NIER 18*. ACM Press. DOI: [10.1145/3183399.3183426](https://doi.org/10.1145/3183399.3183426). URL: <https://doi.org/10.1145/3183399.3183426>.
- Petit, Jonathan and Steven E. Shladover (2014). "Potential Cyberattacks on Automated Vehicles". In: *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11. DOI: [10.1109/tits.2014.2342271](https://doi.org/10.1109/tits.2014.2342271). URL: <https://doi.org/10.1109/tits.2014.2342271>.
- Pichan, Ameer, Mihai Lazarescu, and Sie Teng Soh (June 2015). "Cloud forensics: Technical challenges, solutions and comparative analysis". In: *Digital Investigation* 13, pp. 38–57. DOI: [10.1016/j.diin.2015.03.002](https://doi.org/10.1016/j.diin.2015.03.002). URL: <https://doi.org/10.1016/j.diin.2015.03.002>.
- Pichan, Ameer, Mihai Lazarescu, and Sie Teng Soh (2018). "Towards a practical cloud forensics logging framework". In: *Journal of Information Security and Applications* 42, pp. 18–28. ISSN: 2214-2126. DOI: <https://doi.org/10.1016/j.jisa.2018.07.008>. URL: <https://www.sciencedirect.com/science/article/pii/S2214212617305203>.
- Pollitt, Mark (1995). "Computer forensics: An approach to evidence in cyberspace". In: *Proceedings of the National Information Systems Security Conference*. Vol. 2, pp. 487–491.
- Pollitt, Mark (2010). "A History of Digital Forensics". In: *Advances in Digital Forensics VI*. Springer Berlin Heidelberg, pp. 3–15. DOI: [10.1007/978-3-642-15506-2_1](https://doi.org/10.1007/978-3-642-15506-2_1). URL: https://doi.org/10.1007/978-3-642-15506-2_1.

- Prayudi, Yudi and Azhari SN (Mar. 2015). "Digital Chain of Custody: State of The Art". In: *International Journal of Computer Applications* 114.5, pp. 1–9. DOI: [10.5120/19971-1856](https://doi.org/10.5120/19971-1856). URL: <https://doi.org/10.5120/19971-1856>.
- Qi, Zhengwei, Chengcheng Xiang, Ruhui Ma, Jian Li, Haibing Guan, and David S. L. Wei (2017). "ForenVisor: A Tool for Acquiring and Preserving Reliable Data in Cloud Live Forensics". In: *IEEE Transactions on Cloud Computing* 5.3, pp. 443–456. DOI: [10.1109/TCC.2016.2535295](https://doi.org/10.1109/TCC.2016.2535295).
- Rahman, Nurul Hidayah Ab, Niken Dwi Wahyu Cahyani, and Kim-Kwang Raymond Choo (May 2016). "Cloud incident handling and forensic-by-design: cloud storage as a case study". In: *Concurrency and Computation: Practice and Experience* 29.14, e3868. DOI: [10.1002/cpe.3868](https://doi.org/10.1002/cpe.3868). URL: <https://doi.org/10.1002/cpe.3868>.
- Rahman, Nurul Hidayah Ab, William Bradley Glisson, Yanjiang Yang, and Kim-Kwang Raymond Choo (Jan. 2016). "Forensic-by-Design Framework for Cyber-Physical Cloud Systems". In: *IEEE Cloud Computing* 3.1, pp. 50–59. DOI: [10.1109/mcc.2016.5](https://doi.org/10.1109/mcc.2016.5). URL: <https://doi.org/10.1109/mcc.2016.5>.
- Regulation, General Data Protection (2016). "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46". In: *Official Journal of the European Union (OJ)* 59.1-88, p. 294.
- Ross, Ron, Michael McEvilly, and Janet Carrier Oren (Mar. 2018). *Systems security engineering: considerations for a multidisciplinary approach in the engineering of trustworthy secure systems, volume 1*. Tech. rep. National Institute of Standards and Technology. DOI: [10.6028/nist.sp.800-160v1](https://doi.org/10.6028/nist.sp.800-160v1). URL: <https://doi.org/10.6028/nist.sp.800-160v1>.
- Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid (Nov. 2019). *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*. Tech. rep. National Institute of Standards and Technology. DOI: [10.6028/nist.sp.800-160v2](https://doi.org/10.6028/nist.sp.800-160v2). URL: <https://doi.org/10.6028/nist.sp.800-160v2>.
- Roussev, Vassil (Dec. 2016). "Digital Forensic Science: Issues, Methods, and Challenges". In: *Synthesis Lectures on Information Security, Privacy, and Trust* 8.5, pp. 1–155. DOI: [10.2200/s00738ed1v01y201610spt019](https://doi.org/10.2200/s00738ed1v01y201610spt019). URL: <https://doi.org/10.2200/s00738ed1v01y201610spt019>.
- Rowlingson, Robert (2004). "A ten step process for forensic readiness". In: *International Journal of Digital Evidence* 2.3, pp. 1–28.
- Ruan, Keyun and Joe Carthy (2013a). "Cloud Computing Reference Architecture and Its Forensic Implications: A Preliminary Analysis". In: *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Springer Berlin Heidelberg, pp. 1–21. DOI: [10.1007/978-3-642-39891-9_1](https://doi.org/10.1007/978-3-642-39891-9_1). URL: https://doi.org/10.1007/978-3-642-39891-9_1.
- Ruan, Keyun and Joe Carthy (2013b). "Cloud Forensic Maturity Model". In: *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Springer Berlin Heidelberg, pp. 22–41. DOI: [10.1007/978-3-642-39891-9_2](https://doi.org/10.1007/978-3-642-39891-9_2). URL: https://doi.org/10.1007/978-3-642-39891-9_2.
- Ruan, Keyun, Joe Carthy, Tahar Kechadi, and Ibrahim Baggili (June 2013). "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results".

- In: *Digital Investigation* 10.1, pp. 34–43. DOI: [10.1016/j.diin.2013.02.004](https://doi.org/10.1016/j.diin.2013.02.004). URL: <https://doi.org/10.1016/j.diin.2013.02.004>.
- Ruan, Keyun, Joe Carthy, Tahar Kechadi, and Mark Crosbie (2011). “Cloud Forensics”. In: *Advances in Digital Forensics VII*. Springer Berlin Heidelberg, pp. 35–46. DOI: [10.1007/978-3-642-24212-0_3](https://doi.org/10.1007/978-3-642-24212-0_3). URL: https://doi.org/10.1007/978-3-642-24212-0_3.
- Shapiro, S, N Washington, J Miller, J Snyder, and J McEwen (2014). “Privacy Engineering Framework”. In: *MITRE Privacy Community of Practice*.
- Shields, Clay, Ophir Frieder, and Mark Maloof (Aug. 2011). “A system for the proactive, continuous, and efficient collection of digital forensic evidence”. In: *Digital Investigation* 8, S3–S13. DOI: [10.1016/j.diin.2011.05.002](https://doi.org/10.1016/j.diin.2011.05.002). URL: <https://doi.org/10.1016/j.diin.2011.05.002>.
- Simou, Stavros, Christos Kalloniatis, Stefanos Gritzalis, and Haralambos Mouratidis (Nov. 2016). “A survey on cloud forensics challenges and solutions”. In: *Security and Communication Networks* 9.18, pp. 6285–6314. DOI: [10.1002/sec.1688](https://doi.org/10.1002/sec.1688). URL: <https://doi.org/10.1002/sec.1688>.
- Sjoberg, Katrin, Peter Andres, Teodor Buburuzan, and Achim Brakemeier (June 2017). “Cooperative Intelligent Transport Systems in Europe: Current Deployment Status and Outlook”. In: *IEEE Vehicular Technology Magazine* 12.2, pp. 89–97. DOI: [10.1109/mvt.2017.2670018](https://doi.org/10.1109/mvt.2017.2670018). URL: <https://doi.org/10.1109/mvt.2017.2670018>.
- Svantesson, Dan Jerker B and Lodewijk van Zwieten (2016). “Law enforcement access to evidence via direct contact with cloud providers—identifying the contours of a solution”. In: *Computer Law & Security Review* 32.5, pp. 671–682. DOI: [10.1016/j.clsr.2016.07.011](https://doi.org/10.1016/j.clsr.2016.07.011).
- Svantesson, Dan and Felicity Gerry (2015). “Access to extraterritorial evidence: The Microsoft cloud case and beyond”. In: *Computer Law & Security Review* 31.4, pp. 478–489. DOI: [10.1016/j.clsr.2015.05.007](https://doi.org/10.1016/j.clsr.2015.05.007).
- SWGDE and SWGIT *Digital & Multimedia Evidence Glossary* (2011). Tech. rep. Scientific Working Group on Digital Evidence.
- T-CY (2020a). *Criminal justice access to data in the cloud: challenges*. Accessed: 2020-07-11. URL: <https://rm.coe.int/1680304b59> (visited on 07/11/2020).
- T-CY (2020b). *T-CY assessment report*. Accessed: 2020-07-11. URL: <https://rm.coe.int/16802e726c> (visited on 07/11/2020).
- Tan, John (2001). “Forensic readiness”. In: *Cambridge, MA: @ Stake*, pp. 1–23.
- Times, The New York (2021). *The M.T.A. Is Breached by Hackers as Cyberattacks Surge*. Accessed: 2021-06-08. URL: <https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html> (visited on).
- Trenwith, Philip M and H.S. Venter (Aug. 2013). “Digital forensic readiness in the cloud”. In: *2013 Information Security for South Africa*. IEEE, pp. 1–5. DOI: [10.1109/issa.2013.6641055](https://doi.org/10.1109/issa.2013.6641055). URL: <https://doi.org/10.1109/issa.2013.6641055>.
- Tsai, Wei-Tek, Xin Sun, and Janaka Balasooriya (2010). “Service-Oriented Cloud Computing Architecture”. In: *2010 Seventh International Conference on Information Technology: New Generations*. IEEE. DOI: [10.1109/itng.2010.214](https://doi.org/10.1109/itng.2010.214). URL: <https://doi.org/10.1109/itng.2010.214>.

- Valjarevic, Aleksandar and Hein Venter (2013). "A Harmonized Process Model for Digital Forensic Investigation Readiness". In: *Advances in Digital Forensics IX*. Springer Berlin Heidelberg, pp. 67–82. DOI: [10.1007/978-3-642-41148-9_5](https://doi.org/10.1007/978-3-642-41148-9_5). URL: https://doi.org/10.1007/978-3-642-41148-9_5.
- Vaquero, Luis M., Luis Roderio-Merino, Juan Caceres, and Maik Lindner (Dec. 2008). "A break in the clouds". In: *ACM SIGCOMM Computer Communication Review* 39.1, pp. 50–55. DOI: [10.1145/1496091.1496100](https://doi.org/10.1145/1496091.1496100). URL: <https://doi.org/10.1145/1496091.1496100>.
- Walden, Ian (June 2012). "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent". In: *Computer Communications and Networks*. Springer London, pp. 45–71. DOI: [10.1007/978-1-4471-4189-1_2](https://doi.org/10.1007/978-1-4471-4189-1_2). URL: https://doi.org/10.1007/978-1-4471-4189-1_2.
- Woods, Andrew Keane (2017). "Mutual Legal Assistance in the Digital Age". In: *The Cambridge Handbook of Surveillance Law*. Cambridge University Press, pp. 659–676. DOI: [10.1017/9781316481127.029](https://doi.org/10.1017/9781316481127.029). URL: <https://doi.org/10.1017/9781316481127.029>.
- Yaacoub, Jean-Paul A., Ola Salman, Hassan N. Noura, Nesrine Kaaniche, Ali Chehab, and Mohamad Malli (Sept. 2020). "Cyber-physical systems security: Limitations, issues and future trends". In: *Microprocessors and Microsystems* 77, p. 103201. DOI: [10.1016/j.micpro.2020.103201](https://doi.org/10.1016/j.micpro.2020.103201). URL: <https://doi.org/10.1016/j.micpro.2020.103201>.
- Yahoo (2020). *Yahoo Law Enforcement Guidelines*. Accessed: 2020-07-11. URL: <https://www.verizonmedia.com/transparency/about/faq-glossary.html> (visited on 07/11/2020).
- Zammad (2020). *Zammad Community*. Accessed: 2020-07-11. URL: <https://www.zammad.org> (visited on).
- Zawoad, Shams, Amit Kumar Dutta, and Ragib Hasan (Mar. 2016). "Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service". In: *IEEE Transactions on Dependable and Secure Computing* 13.2, pp. 148–162. DOI: [10.1109/tdsc.2015.2482484](https://doi.org/10.1109/tdsc.2015.2482484). URL: <https://doi.org/10.1109/tdsc.2015.2482484>.
- Zawoad, Shams and Ragib Hasan (Mar. 2016). "Trustworthy Digital Forensics in the Cloud". In: *Computer* 49.3, pp. 78–81. DOI: [10.1109/mc.2016.89](https://doi.org/10.1109/mc.2016.89). URL: <https://doi.org/10.1109/mc.2016.89>.

Résumé

Les inventions pervasives, et autres technologies labellisées Smart, reposent sur les ressources que procurent les services de l'informatique en nuage. Ceci dit, les incidents de sécurité ou cybercrimes se produisent. Plus que ça, la probabilité qu'un incident numérique ait un impact sur des objets physiques n'est plus négligeable. L'investigation légale numérique lors de l'occurrence d'un incident de sécurité ou cybercrime dans de tels environnements est complexe. Les cyber-criminologistes font face à de multiples challenges tels que la multitenancy et les juridictions multiples. Ces derniers ne sont que des exemples de challenges parmi d'autres de l'investigation légale numérique dans les systèmes basés sur l'informatique en nuage . Préparer ces écosystèmes émergents à accueillir une investigation légale numérique et maximiser leurs potentiel à fournir des évidences numériques est encore plus complexe, d'où la nécessité d'un changement de perspective. Cependant, concevoir de nouveaux systèmes ayant la capacité à fournir des évidences numériques dès la conception en adoptant une stratégie dite Forensic-by-design peut être attrayant, mais son inefficacité dans les systèmes qui reposent sur l'informatique en nuage est prouvée. Dans cette thèse, une amélioration de ce concept et un framework sont proposés et validés. L'évaluation du potentiel de la nouvelle approche dans le contexte des systèmes de transport intelligents est ensuite menée. Finalement, le problème des juridictions multiples est abordé et une solution est proposée pour la gestion des injonctions judiciaires qui permet l'accès aux représentants de la loi aux évidences numériques dans les systèmes basés sur l'informatique en nuage .

Mots clefs: Investigation légale numérique, Informatique en nuage, préparation à l'investigation légale numérique, aptitude à l'investigation par conception, juridictions multiples, force de l'ordre .

Abstract :

Pervasive innovations and Smart labeled technologies are backed by flexible, ubiquitous, scalable and on demand computing resources served through Cloud computing services. However, security incidents and cybercrime happen. Moreover, the likelihood of a digital incident having an impact on physical assets is no more negligible. A Digital Forensic Investigation of the occurrence of a security incident or cybercrime in such an emergent ecosystem is challenging. Cyber-Criminalists are facing multiple challenges, such as multi-tenancy and multi jurisdictions which are some examples of the Cloud Forensics issues. Furthermore, enabling these new Cloud computing backed environments with the due capabilities —Cloud Forensic Readiness— that will maximize their ability to collect digital evidence is even more challenging. A shift in perspective is therefore required. While aiming towards the design of a forensic-ready system by adopting a Forensic-by-Design strategy seems interesting, However, its inefficiency in Cloud computing environments is proven. In this work. An improved framework for Forensic-by-Design Cloud computing system is proposed and validated. The assessment of a Forensic-ready Intelligent Transportation System is investigated as a validation of the proposed vision. Finally, multi-jurisdictions and Law Enforcement access to digital evidence in the Cloud is investigated and a Cloud Law enforcement Request Management System is proposed.

Keywords: Digital Forensics, Cloud Forensics, Cloud Forensics Readiness, Forensic-by-design, ForensicReady, Multi-Jurisdictions, Law Enforcement.

الملخص:

الابتكارات واسعة الانتشار والتقنيات التكنولوجية الذكية مدعومة بوسائل حوسبة مرنة وواسعة الانتشار وقابلة للتطوير وعند الطلب، يتم تقديمها من خلال خدمات الحوسبة السحابية. ومع ذلك، تقع حوادث أمنية وجرائم إلكترونية. بالإضافة إلى ذلك، فإن احتمال وقوع حادث رقمي له تأثير على موارد مادية لم يعد مهملاً. يعد التحقيق الجنائي الرقمي في وقوع حادث أمني أو جريمة إلكترونية في مثل هذا النظام البيئي الناشئ أمراً صعباً. تدعيم البيانات الجديدة القائمة على الحوسبة السحابية بالإمكانات الواجبة والتي ستزيد من قدرتها على جمع الأدلة الرقمية يعد أمراً أكثر صعوبة. لذلك فإن التغيير في المنظور ضروري. في حين أن الهدف من تصميم نظام جاهز للتحقيق الجنائي الرقمي من خلال التصميم ومن خلال اعتماد استراتيجية التحقيق الجنائي الرقمي حسب التصميم يبدو مثيراً للاهتمام، لكن ثبت عدم كفاءته في بيئة الحوسبة السحابية. في إطار هذه الذاكرة يتم اقتراح نظام للتحقيق الجنائي الرقمي من خلال التصميم في بيئة الحوسبة السحابية ويتم التحقق من صحته من خلال تقييمه في نظام النقل الذكي. أخيراً، يتم التحقيق في الاختصاصات القضائية المتعددة ووصول جهات إنفاذ القانون إلى الأدلة الرقمية في السحابة ويتم أيضاً اقتراح نظام إدارة طلبات إنفاذ القانون عبر السحابة.

الكلمات الرئيسية: التحقيق الجنائي الرقمي، التحقيق الجنائي الرقمي السحابي، جاهزية التحقيق الجنائي الرقمي، التحقيق الجنائي الرقمي حسب التصميم، الاختصاصات المتعددة، إنفاذ القانون.