2020

Ontology-driven perspective of CFRaaS

Victor R. Kebande

Nickson M. Karie
Edith Cowan University

Richard A. Ikuesan

Hein S. Venter

10.1002/wfs2.1372
Kebande, V. R., Karie, N. M., Ikuesan, R. A., & Venter, H. S. (2020). Ontology-driven perspectives of CFRaaS. *WIREs Forensic Science, 2*(5), article e1372. https://doi.org/10.1002/wfs2.1372

Received: 29 September 2019 | Revised: 13 February 2020 | Accepted: 14 February 2020

DOI: 10.1002/wfs2.1372

FOCUS ARTICLE

WIREs FORENSIC SCIENCE WILEY

Ontology-driven perspective of CFRaaS

Victor R. Kebande[1] | Nickson M. Karie[2] | Richard A. Ikuesan[3] | Hein S. Venter[4]

[1]Department of Computer Science and Media Technology, Malmö Universitet, Nordenskiöldsgatan, Malmö, Sweden

[2]ECU - Security Research Institute, Faculty of Science, Edith Cowan University, Joondalup Campus, Joondalup, Western Australia, Australia

[3]Department of Cybersecurity and Networking, School of Information Technology, Community College of Qatar, Doha, Qatar

[4]DigiFORs Research Group, Department of Computer Science, University of Pretoria, Pretoria, South Africa

Correspondence
Victor R. Kebande, Department of Computer Science and Media Technology, Malmö Universitet, Nordenskiöldsgatan, Malmö, Sweden.
Email: victor.kebande@mau.se

Nickson M. Karie, ECU - Security Research Institute, Faculty of Science, Edith Cowan University, Joondalup Campus, WA, Australia.
Email: nickson.karie@gmail.com

Richard A. Ikuesan, Department of Cybersecurity and Networking, School of Information Technology, Community College of Qatar, Doha, Qatar.
Email: rikuesan@gmail.com

Abstract

A Cloud Forensic Readiness as a Service (CFRaaS) model allows an environment to preemptively accumulate relevant potential digital evidence (PDE) which may be needed during a post-event response process. The benefit of applying a CFRaaS model in a cloud environment, is that, it is designed to prevent the modification/tampering of the cloud architectures or the infrastructure during the reactive process, which if it could, may end up having far-reaching implications. The authors of this article present the reactive process as a very costly exercise when the infrastructure must be reprogrammed every time the process is conducted. This may hamper successful investigation from the forensic experts and law enforcement agencies perspectives. The CFRaaS model, in its current state, has not been presented in a way that can help to classify or visualize the different types of potential evidence in all the cloud deployable models, and this may limit the expectations of what or how the required PDE may be collected. To address this problem, the article presents the CFRaaS from a holistic ontology-driven perspective, which allows the forensic experts to be able to apply the CFRaaS based on its simplicity of the concepts, relationship or semantics between different form of potential evidence, as well as how the security of a digital environment being investigated could be upheld. The CFRaaS in this context follows a fundamental ontology engineering approach that is based on the classical Resource Description Framework. The proposed ontology-driven approach to CFRaaS is, therefore, a knowledge-base that uses layer-dependencies, which could be an essential toolkit for digital forensic examiners and other stakeholders in cloud-security. The implementation of this approach could further provide a platform to develop other knowledge base components for cloud forensics and security.

This article is categorized under:
Digital and Multimedia Science > Cloud Forensics
Digital and Multimedia Science > Cyber Threat Intelligence
Digital and Multimedia Science > Multimedia Forensics

KEYWORDS

CFRaaS, cloud, comparative, digital, forensic, model, ontology, readiness-as a service

1 | INTRODUCTION

The rapid decline in traditional digital forensics (DF) practice has enabled the field of cloud forensics to have numerous advances and most importantly, digital investigation in the cloud resources, which has been at the center of these advances. This has been influenced by the increased complexity of attack tools, and cyber-attack techniques, improved anti-forensic strategies and the quest for attribution (Alruban, Clarke, Li, & Furnell, 2017; Ikuesan & Venter, 2017, 2019). Often, the cloud forensics discipline, which is an amalgamation of DF and cloud computing, relies on purely extracting evidentiary digital artifacts from the cloud environment, which in real cases is open and distributed in nature. This openness of the cloud and it is on demand-resources has mainly been the driving force behind increased adversarial attacks. Generally, digital forensic processes in the cloud are ever-growing because of the necessity to prove that a digital crime or a security incident occurred at a given point in the cloud. Also, another aspect to ponder on is the fact that digital crimes are electronic and the regular changes in technology mean that the digital investigation approaches and techniques are bound to change as well. It is also important to note that, the Law Enforcement Agencies (LEAs) and digital forensic experts (DFE) are on each day faced with investigation challenges due to the proliferation of digital devices and the increased volumes of digital evidence (Slay & Schulz, 2014).

The Cloud Forensic Readiness as a Service (CFRaaS) model which is aimed at shortening the digital investigation process in the cloud environment was developed in a manner, that allows it to accumulate potential digital evidence (PDE) irrespective of volume and file formats of the artifacts from the cloud environment in a timely fashion. The advantage of using CFRaaS is that it maximizes the time that may be needed to conduct a digital forensic investigation (DFI), while at the same time it ensures that there are limited chances of tampering, alteration or modification of the cloud infrastructures and also it saves the cost of conducting a DFI. The authors posit that in different instances, it may be possible to find sources of alterations if an alteration or tampering is attempted. Note that tampering or altering in the context of this research shows various techniques that help in preserving the integrity of the accumulated digital evidence from the cloud environment. Given that cloud nodes have a possibility of belonging to different users (Delport, Köhn, & Olivier, 2011) when information or evidence is collected as per the guidelines mentioned in ISO/IEC 27043 on evidence that is collected, hashing or the creation of cryptographic hashes is preferred. While this is only subjected to the collected evidence, it is worth mentioning that, this sanctity of evidence allows noninterference with other cloud infrastructures or systems thereof. This is because the accumulated PDE is removed from the cloud for further analysis (Kebande & Venter, 2018). Important to mention also, is the fact that, while these forensic processes are being conducted, the chain of custody is preserved at the same time (Kebande & Venter, 2019). Additionally, the CFRaaS is presented as a novel concept that is able to pinpoint the sources of electronic evidence, gathering evidence based on the forensic readiness steps that have been mentioned by (Rowlingson, 2004) as well as the guidelines that are mentioned in the ISO/IEC 27043:2015 International standards. While ISO/IEC 27043 advocates for or presents an umbrella standard for high-level concepts of digital investigation, it is important to note that CFRaaS tries to address preemptive strategies that can be important for risk mitigation approaches in organizations.

Currently, there exist some research gaps on how to represent cloud forensic processes and how to semantically generate some reasoning based on the tasks that are achieved by CFRaaS. Consequently, this study explores the complexity of the cloud environment and the challenges that may exist while conducting DFIs and CFRaaS has been used as a basis for this study. Based on this, it is also important to highlight that, there is a need to model CFRaaS using ontology approaches in order to address the prevailing cloud security challenges. As a result, an explicit conceptualizations of CFRaaS is needed to help digital investigators and the LEAs to be able to manage knowledge. This allows different actors to have a common or shared understanding of CFRaaS. Furthermore, this lack of knowledge management process has also limited the knowledge discovery within the CFRaaS. Knowledge discovery in this regard provides a baseline for digital investigators and LEAs to explore the underlying relationships among forensic attributes in the cloud. Such is important in a dynamic platform where novel routing, data management, and data communication are constantly deployed. In addition, the dynamic composition of the threat landscape and threat actors requires a standardized approach that uses ontologies to map the CFRaaS processes. In order to realize the CFRaaS processes integration to ontologies, a methodology that is robust toward a dynamic landscape is required. Studies have expounded on the suitability of an ontology-driven approach to address such research problems (Karie & Venter, 2014). An ontology-driven model, as further expounded in the subsequent sections of this research article, is a step-by-step modeling approach that reveals structural dependencies among observable attributes in each knowledge area based on succinct logic (description logic), for all probable stakeholders. By leveraging the knowledge base provided by the ontology-driven modeling approach to knowledge management, this study, therefore, proposes a novel robust ontology-based CFRaaS that can be used by both digital investigators, and LEAs. More so, the ontology-driven perspective of CFRaaS that has been proposed in this article can help to bring out some in-depth concepts, features, and objects that may be useful while applying CFRaaS to a typical investigative scenario.

The authors give the contribution of this article as follows:

1. Model the CFRaaS from an ontology-driven perspective based on layer(process) dependencies
2. Provide comprehensive representation and mapping of CFRaaS processes from an ontology point of view
3. Generate a contextual discussion based on the propositions

The remainder of this article is organized as follows: In Section 2, a preliminary study of CFRaaS is given while its associated processes are presented in Section 3. Related work is covered in Section 4. This is followed by ontology modeling processes in Section 5 and the ontology-driven perspective of CFRaaS is given in Section 6. A comparative approach of CFRaaS and other existing ontology-based models is given in Section 7 while discussion and evaluation of the propositions are given in Section 8. A conclusion and a mention of the future work of the study are given in Section 9.

2 | PRELIMINARY WORK ON CFRAAS

A CFRaaS model is presented as a novel implementation that has been deployed in a cloud environment in order to be able to achieve Digital Forensic Readiness (DFR) by maximizing the potential of using PDE while minimizing the cost of conducting DF investigations. This concept stems from the dire need for shortening the DFI process across organizations. Apart from that, being a preemptive implementation, this concept attempts to address organization's risk management and mitigation strategies at the same time having to prevent to reprogram the cloud infrastructure, which is mainly a costly exercise and, in most cases this may end up have far-reaching implications (Kebande & Venter, 2018) during digital investigations. Consequently, the implementation of CFRaaS and its associated processes (layers) conforms and translates into the guidelines that have been mentioned in ISO/IEC 27043 international standard, which deals with Information Technology (IT), Security Techniques, Incident Investigation Principles, and Processes. Notably, the unique CFRaaS recurring processes have allowed this model to specifically be a suitable approach to achieving or prepare the cloud environment for DFR. Apart from that, CFRaaS has been presented as a proactive process that openly focuses on pre-incident strategies that allow the Cloud Service Providers (CSPs) to be able to manage forensic activities by employing software agents (Kebande & Venter, 2014). These software agents are a modified form of botnets and can collect useful information in a digital forensic manner that may be used as PDE during litigation if a potential security incident is detected.

CFRaaS consists of five main processes namely: *provider layer, virtualization layer, DFR layer, Incident Response Procedure (IRP) layer*, and the *concurrent processes layer*. According to research conducted by Kebande and Venter (2019)), the DFR layer and the concurrent process layer strictly adheres to the guidelines of ISO/IEC 27043 international standard while IRP is presented as a reactive process which is a post-event response process. Nevertheless, each of the layers that have been mentioned has different roles. For example, the provider layer acts as a gateway through which services are provided by the CSPs through the virtualization layer. Thereafter, useful DFI can easily be captured through the DFR layer. An important aspect that has been employed is the deployment of botnets in a non-malicious approach. Botnets, which have been used as software agents, have been modified to be able to collect information and report to the botnet operator, digitally preserve this information in preparation for a DFI. While the pragmatic connotation of employing botnets has not directly been mentioned as a process in ISO/IEC 27043, it forms one of the most important and novel aspects of this research, owing to the fact that, the initially considered malicious botnets are transformed to collect digital information without any negative connotation. Next, the concurrent processes that have been taken verbatim from ISO/IEC 27043 have been employed in tandem with other digital forensic processes that have been mentioned in the CFRaaS. The importance of employing the concurrent processes in CFRaaS, is mainly for these processes to be able to increase the chances of achieving admissibility for the collected PDE during litigation. Figure 1 shows the detailed CFRaaS model with the main processes and subprocess. The role of each of the subprocess has subsequently been explained as shown in Table 1.

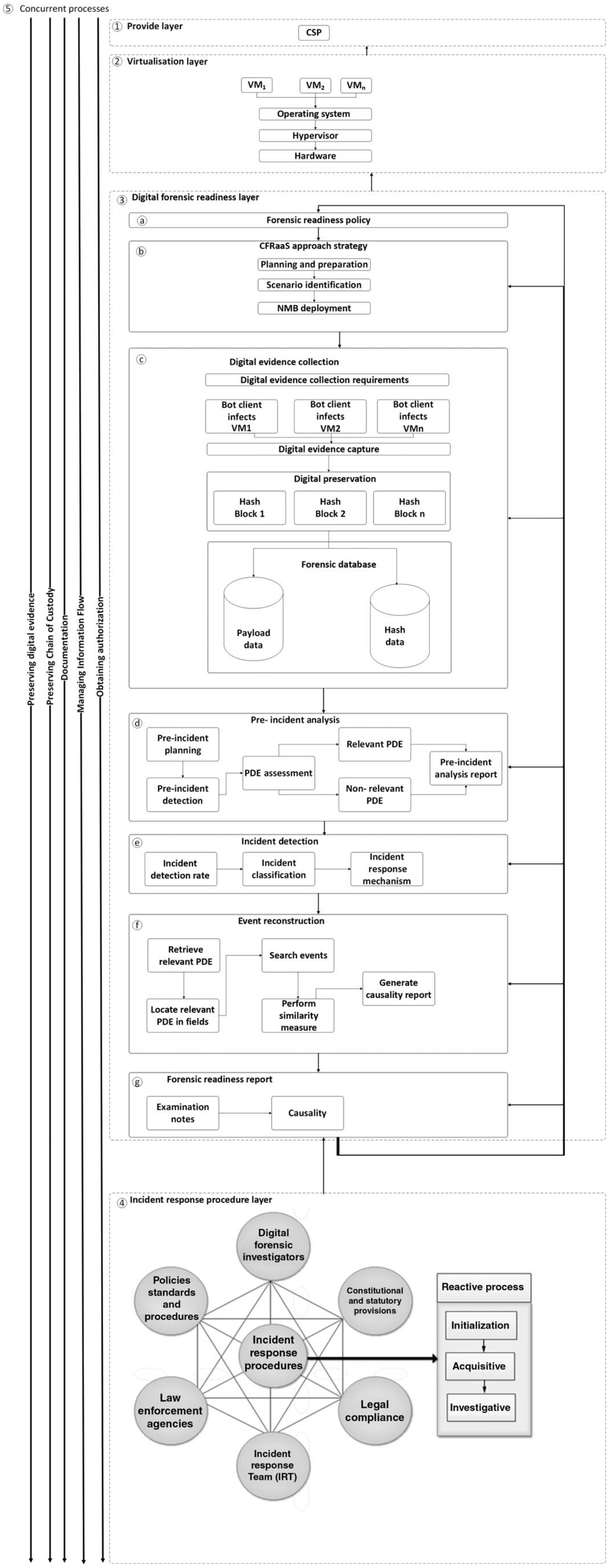


FIGURE 1 CFRaaS process flow (Kebande & Venter, 2018). CFRaaS, Cloud Forensic Readiness as a Service

TABLE 1 CFRaaS main processes, subprocesses, and functions

	CFRaaS process	CFRaaS subprocess		Function
1	Provider layer	*Cloud service provider (CSP)*		Provide services over the internet
2	Virtualization layer	a	*Virtual machine*	Enables virtualization
		b	*Hypervisor*	Software management
		c	*Operating system*	Instance support
		d	*Hardware*	Software support
3	Digital forensic readiness layer	a	*Forensic readiness policy*	Ensure legal premise is admissible
		b	*CFRaaS approach strategy*	Define processes to collect by CSPs evidence
		c	*Digital evidence collection*	Technique used to collect digital evidence
		d	*Pre-incident analysis*	Reviewing collected potential digital evidence
		e	*Incident detection*	Identification of security incidents
		f	*Event reconstruction*	Trace and examine previously occurred events
		g	*Forensic readiness report*	Interpretation of forensic readiness results
4	Incident response procedure layer	*Reactive process*		Conducting digital forensic investigations through a post-event response approach
5	Concurrent processes	*Simultaneous processes*		Ensures admissibility is maintained

Abbreviation: CFRaaS, Cloud Forensic Readiness as a Service.

3 | CFRaaS PROCESSES

The underlying complexities and existing cloud forensic challenges across different cross-cutting jurisdictions have paved the way for the proposition of CFRaaS. CFRaaS which is a proactive model provides a holistic technique that mainly aims to achieve DFR in the cloud environment. Nevertheless, the CFRaaS processes allow the cloud to be forensically ready for the post-event response processes. From Figure 1, this has been represented as an IRP process. However, Table 1 shows a summary of the main CFRaaS processes, respective subprocesses and the function of each of the subprocess that has been mentioned. A more detailed CFRaaS model is shown in Figure 1 with processes that are implemented as part of the DFR approach. Important aspects that have been realized by the processes that have been mentioned in Table 1 include the collection of digital forensic information, creating a cryptographic hash of each of the collected block of digital evidence in order to preserve the integrity of the collected information and then storing this information in a forensic database in preparation of post-event response processes.

The *Provider layer* which has the CSP service decommissioning sub-process has been presented in Layer 1. This is followed by *Virtualization Layer* with VM support and implementation process that supports different instance deployment, a hypervisor that manages the cloud operating system, the operating system that supports instance creation and hardware that represents the physical processes that support cloud infrastructures. This is followed by the DFR Layer that has a forensic readiness policy that ensures that the legal premise is admissible, CFRaaS approach strategy that defines the processes used to collect digital evidence through the digital evidence collection subprocess.

This is then followed by a *Pre-incident Analysis* process that involves a proper review of collected digital evidence. Identification of security incidents is achieved in the incident detection process and events that transpired during the process are recapped through event reconstruction processes. The interpretation of the forensic readiness results is achieved by a forensic readiness report. This is followed by the IRP layer that acts as a post-event response process. Finally, the concurrent processes that happen simultaneously to ensure that the admissibility of potential digital shreds of evidence is maintained while the processes are being conducted.

4 | RELATED WORK

Generally, the premise of creating ontologies for cloud forensic readiness models is least explored at the time of writing this research article. CFRaaS stands out to be a holistic approach for achieving DFR in a complex cloud environment. Thus, in this section, the authors present some relevant works that be referred to as related work. Research on digital forensic ontologies by (Park, Cho, & Kwon, 2009) mainly focused on investigating digital crimes in cyberspace. From the research work, the investigation and research community can articulate a taxonomical structure of various cybercrime concepts and the relationships that exist among the different types of crimes, digital evidence collection, criminal cases, and the law. Although the model by these researchers explores various processes on digital evidence such as collection, identification, searching, transportation, storage, and examination, their ontology hardly identifies approaches that could be used to map the processes to the cloud.

Similarly, studies by Ellison and colleagues (Ellison, Ikuesan, & Venter, 2019; Ellison, Venter, & Ikuesan, 2017) explored the potential of developing a holistic digital forensic knowledge base which can be applied within the general field of DF. The Authors presented a forensic ontology and the corresponding description logic and axiom that can be used to functionally implement the presented ontology. It suffices to note that the proposition presented by these studies targets a generic knowledge base for DF without a specific concept to cloud forensics. In this regard, cloud forensics was subsumed under network and computer forensics, which has long been dichotomized. This singular point of failure thus provided a foundational background and the need for a cloud-based knowledge base that can be leveraged to classify and model cloud forensics. A knowledge base is a technology used to explore complex information such that a computer system can glean knowledge to perform an informed decision-making process (Raad & Cruz, 2015).

Next, is a framework called DIALOG was conceptualized to encapsulate the different concepts in DF as well as the relationship between those specific concepts. This framework has been able to reuse digital forensic knowledge that is associated with digital investigation cases (Kahvedžić & Kechadi, 2009). Another research on building ontologies for digital forensic terminologies by (Karie & Kebande, 2016) focused on establishing approaches that could help in the reasoning process during digital investigation, specifically with respect to digital forensic terminologies. This has been achieved by the conceptualization of an ontological approach that can be used to resolve the meaning of those terminologies. Again, research by Karie and Venter (2014) developed a general ontology for digital forensic disciplines that can aid in the development of the methodologies and specifications that can offer direction in different areas of DF. Other relevant research includes a cyber forensic ontology by Brinson, Robinson, and Rogers (2006) that addresses education and specialization aspects in the cyber forensic domain. Research by Slay and Schulz (2014) further conceptualized other use of ontologies as a technique for examining evidence using software filters. These related researches attempted to provide one perspective of ontology as it relates to DF, albeit from a generic view, without specific consideration to cloud-based ontological reasoning. Given that technological advances is gradually navigating toward a cloud-based computing dispensation, it is logical to pre-empt that crimes could likely follow similar migration. There is therefore a need to consider approaches that relates specifically to crime control, ultimate approaches to crime prevention in the cloud domain.

5 | ONTOLOGY MODELING OF THE PROPOSED CFRaaS

Ontology methodology generally comprises the steps adopted to develop and evaluate a given ontology. This study, therefore, follows a similar logic, which typically aligns with the knowledge engineering approach and mixed method of research evaluation. To model the domain of CFRaaS, this study adopted the fundamental logic of ontology engineering which comprises stakeholder identification and definition, term enumeration and elicitation from respective stakeholders, competency question derivation, axiom formation, and deductive reasoning, as well as class and hierarchy extraction. An iterative design approach was considered for this engineering process. In order to ascertain the viability of the proposed modeling approach, a preliminary evaluation process is developed. This evaluation process utilized the classical Resource Description Framework (RDF). Expert opinion on the classes and the semantic relationship among CFRaaS terminologies considered as the evaluation mechanism for the feasibility of the proposed ontological approach to CFRaaS knowledge representation. This is further examined using a probable use-case review process. Taken together, the ontology modeling and integration constitute the thematic analysis and evaluation of this study.

6 | ONTOLOGY-DRIVEN PERSPECTIVE OF CFRaaS

6.1 | Modeling of CFRaaS

The logic of ontology opines that a known relationship among multiple variables and/or features can be modeled such that the dependencies and interdependencies can be categorically stated without ambiguity. In such cases, the underlying adjectival connectivity between two variables can reveal the functionality and potential output of the relationship. The output from such a process can then be formally depicted for machine readability and knowledge base implementation. Basically, ontology modeling defines the conceptual structure that is used to represent the ontology data (Knowledge). Ontology modeling is also a kind of knowledge representation method and the knowledge is represented as an ontology as described in the subsequent sections.

6.2 | Layer dependencies in CFRaaS

According to (Delugach, Cox, & Skipper, 2016) "Dependency" is any situation involving two or more elements such that a change in one or more elements leads to a potential change in one or more other elements. In this section, the authors try to show the dependencies based on the CFRaaS layers proposed. Figure 2 below shows how the different CFRaaS layers are interlinked with each other. A change in the concurrent processes layer, for example, will affect all other layers in the model. In the authors' opinion, presenting the dependencies as shown in Figure 2 was necessary to simplify the understanding of the CFRaaS Layer dependencies as well as to present specific finer details. Each of the layers as shown in Figure 2 are briefly discussed in context in the sections to follow.

6.2.1 | Provider layer

The provider layer is like an interface between the services offered by different service providers over the Internet and the clients. In this layer, servers which host all the services and owned by the service provider are provisioned to different cloud clients based on the agreed service level agreements. The provider layer, therefore, takes care of such things as convenient, secure, and reliable services. From an otology perspective, this layer and all its services can be modeled effectively using some ontology modeling language to form a knowledge base representation. This will enable different service providers to share a common understanding of the CFRaaS layers. To put this in context, taking the Provider layer as an instance type then all the services can be treated as subtypes of the instance type as shown in Figure 3. Not that, the main components of an ontology are concepts, relations, instances, and axioms. A *concept* represents a set or class of entities or "things" within a domain. The r*elations* describe the interactions between concepts or a concept's properties while the *Instances* are the "things" represented by a concept and the *axioms* are used to constrain values for classes or instances.

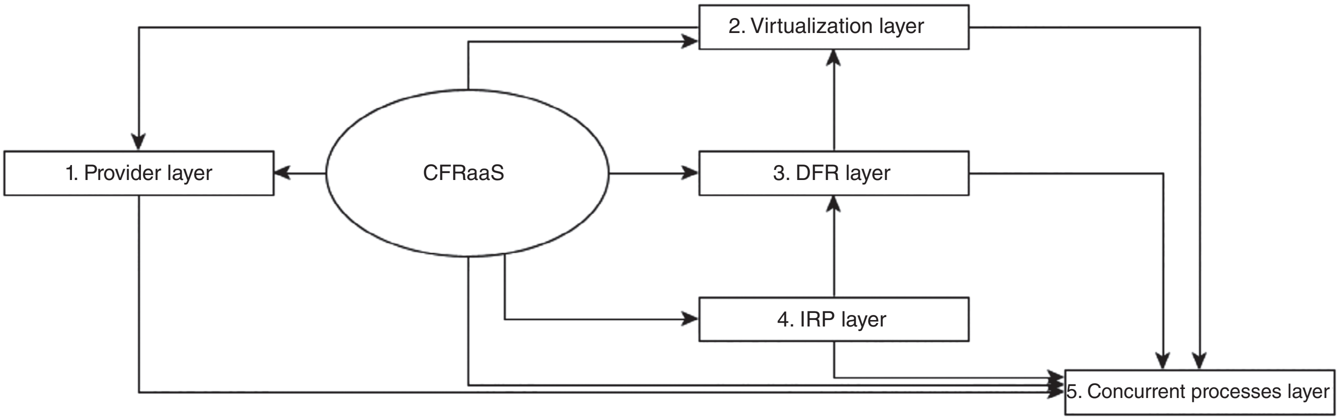


FIGURE 2 Layer-dependencies in CFRaaS. CFRaaS, Cloud Forensic Readiness as a Service

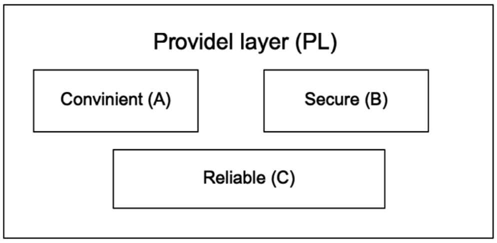


FIGURE 3 Instance and sub-instance type of the provider layer

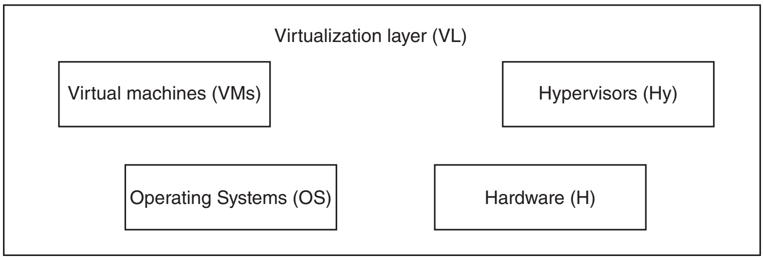


FIGURE 4 Instance and sub-instance type of the virtualization layer

Using the RDF, which is part of the ontology languages proposed for the Semantic Web; the instances as shown in Figure 3 can then be treated as subject or predicates and the sub-instances can be treated as objects. Subjects and predicates are usually treated as resources while objects are either resources or literals (constants). Further RDF Schema (RDFS) can also be used to build on RDF by adding formal support for classes and sub-classing.

This means that RDFS supports specialization and sub-setting of predicates. In this context, therefore, using "⊆" for "is a sub-type of," "&" for "AND," and "→" for "implies," then we can write the relationships shown in Figure 3 as:

(Convenient Services (A) & Secure Services (B) & Reliable Services (C)) ⊆ Provider Layer (PL.)

However, further inferences may be drawn by using the rdf: type and rdfs: subClassOf predicates in combination as shown below. For example, using "∈" for "is an instance of" and "⊆" for "is a subclass of" as is shown in Equation (1):

$$A \in PL \,\&\, B \in PL \,\&\, C \in PL \rightarrow (A \,\&\, B \,\&\, C) \in PL. \tag{1}$$

This can be expressed in terms of subclasses as below as shown in Equation (2).

$$A \subseteq PL \,\&\, B \subseteq PL \,\&\, C \subseteq PL \rightarrow (A \,\&\, B \,\&\, C) \subseteq PL \tag{2}$$

This process can then be repeated for all layers taking into consideration all the subjects or predicates and the sub-instances.

6.2.2 | Virtualization layer

In a cloud environment, virtualization can be used to mean the act of creating a virtual version of something, including virtual computer hardware platforms, storage devices, and computer network resources. In the case of the CFRaaS, virtualization is used to provide a separation of the virtual machines from the physical infrastructure. This concept thus allows PDE to be collected from different virtual machines, operating systems, hypervisors, and hardware. The detailed concepts of some of these activities are explained in Section 6.3 which handles the ontological modeling concepts. Figure 4 shows the instance and the instance type of the virtualization layer.

Therefore, from Figure 4 as explained earlier, using "⊆" for "is a sub-type of," "&" for "AND," and "→" for "implies," we can infer that:

$$(\text{Virtual Machine (VM)} \,\&\, \text{Hypervisors (HY)} \,\&\, \text{Operating Systems (OS)} \,\&\, \text{Hardware (H)}) \subseteq \text{Virtualization Layer (VL)}. \tag{3}$$

However, using "∈" for "is an instance of" and "⊆" for "is a subclass of" then:

$$VM \in VL \,\&\, HY \in VL \,\&\, OS \in VL \,\&\, H \in VL \rightarrow (VM \,\&\, HY \,\&\, OS \,\&\, H) \in VL \tag{4}$$

This can be expressed in terms of sub-classes as is shown in Equation (5).

$$VM \subseteq VL \,\&\, HY \subseteq VL \,\&\, OS \subseteq VL \,\&\, H \subseteq VL \rightarrow (VM \,\&\, HY \,\&\, OS \,\&\, H) \subseteq VL \tag{5}$$

6.2.3 | DFR layer

The DFR layer takes care of forensic readiness policy (FRP), CFRaaS approach strategy (CAS), digital evidence collection (DEC), pre-incident analysis (PIA), incident detection (ID), event reconstruction (ER), and forensic readiness report (FRR). In this layer just like the previous layers, we infer that, "⊆" for "is a subtype of," "&" for "and," and "→" for "implies," hence we can infer that:

$$(FRP \,\&\, CAS \,\&\, DEC \,\&\, PIA \,\&\, ID \,\&\, ER \,\&\, FRR) \subseteq DFR \tag{6}$$

However, using "∈" for "is an instance of" and "⊆" for "is a subclass of' then:

$$\begin{aligned} &FRP \in DFR \,\&\, CAS \in DFR \,\&\, DEC \in DFR \,\&\, PIA \in DFR \,\&\, ID \in DFR \,\&\, ER \in DFR \,\&\, FRR \in DFR \\ &\quad \rightarrow (FRP \,\&\, CAS \,\&\, DEC \,\&\, PIA \,\&\, ID \,\&\, ER \,\&\, FRR) \in DFR \end{aligned} \tag{7}$$

This can be expressed in terms of subclasses as below:

$$\begin{aligned} &FPR \subseteq DFR \,\&\, CAS \subseteq DFR \,\&\, DEC \subseteq DFR \,\&\, PIA \subseteq DFR \,\&\, ID \subseteq DFR \,\&\, ER \subseteq DFR \,\&\, FRR \subseteq DFR \\ &\quad \rightarrow (VFRP \,\&\, CAS \,\&\, DEC \,\&\, PIA \,\&\, ID \,\&\, ER \,\&\, FRR) \subseteq DFR \end{aligned} \tag{8}$$

6.2.4 | IRP layer

The IRP layer comprise of DF investigators, policies, standards and procedures, LEAs, incident response teams, legal compliance, constitutional, and statutory provisions as well as the reactive processes. Just like the previous Layers, Using "⊆" for "is a subtype of," "&" for "AND," and "→" for "implies," as well as "∈" for "is an instance of' and "⊆" for "is a subclass of' then one would model this layer in the same way. In doing this, one creates an environment where knowledge can be shared with the help of ontologies.

6.2.5 | Concurrent processes layer

The concurrent processes as shown in Figure 2 are meant to be executed alongside all the other processes. They provide a good way of handling digital evidence to enable a holistic approach to the DFI process. The main goal of these processes according to Valjarevic and Venter (2015) is to ensure the admissibility of digital evidence in a legal system (ISO/IEC 27043).

The tasks involved in concurrent processes according to ISO/IEC 27043 standard include documentation, managing information flow, obtaining authorization, preservation of chain of custody, and digital evidence. Documentation involves taking notes based on the outcome of the digital investigation process while information flow allows automation of ongoing processes. Obtaining authorization, on the other hand, is done after a security incident has been detected and allows an interaction that can enable a forensic administrator to perform activities dealing with physical investigations. The chain of custody shows the roadmap of the preservation of digital evidence and how each form of evidence is collected even when changes are made. Digital preservation of the collected evidence is done through hashing to maintain evidence in its original form. Hashing transforms and generates values from the collected PDE using mathematical functions in order to help retain collected evidence in its original form.

6.3 | Compliance of CFRaaS ontology with ISO/IEC 27043 Standard

Ontology in digital investigation and forensics, as described in (Ellison et al., 2017; Ellison et al., 2019), is the formal approach of representing digital forensic attributes in a manner that presents effective knowledge base representation. Such representation typically encompasses the contextual inter-connectivity of attributes, viewed from different stakeholder's perspectives. As asserted in existing ontology studies (Karie & Kebande, 2018; McGuinness & Noy, 2000), two (among the four fundamental components of ontology) justification for ontological reasoning; the need to share a common understanding of structures within the CFRaaS knowledge domain, and the need to make assumptions and interconnectivity, explicit. Leveraging ontological reasoning of a knowledge base for CFRaaS, therefore, requires a holistic paradigm of identifying, defining and formally describing the composition of each attribute within the CFRaaS domain. An extrapolated development lifecycle for CFRaaS using ontological concept and reasoning is presented in Figure 5. As depicted in Figure 5, the CFRaaS ontology-based modeling lifecycle involves a closed iterative process. The termination stage of the modeling process can be carried out by the stakeholder at any stage of the modeling process. The lifecycle considers the various components required to effectively integrate knowledge base into cloud forensics. It comprises the identification and clarification of stakeholders for the CFRaaS domain. Stakeholders in this context refer to “the who” that can be involved in CFRaaS, which can include human actors who can use cloud forensics (the forensic investigators, and LEAs for instance), who can develop cloud-based solutions (the cloud service providers for instance). This can be logically reasoned to include consumers of cloud services. However, such inclusion would require a further granular definition of cloud service consumer categories.

This lifecycle further shows an iterative process between the stakeholder identification and stakeholder requirement specification. Although requirements could vary from one stakeholder to another, it is logical to assume that, at the high-level, the general requirement falls within the cloud computing platform. This further provides a baseline for knowledge reuse from one stakeholder to another, context notwithstanding. Context-dependent requirements introduce the specification from different stakeholders which utilizes the cloud platform terminology. Terminology enumeration involves the identification and definition of the various concepts and terms associated with the cloud platform, usually from the stakeholder's perspective. Concepts in this regard can be the various service models of a typical cloud service such as IaaS, PaaS, as well as SaaS. The associated terminologies for each of the identified concepts, as well as service-specific terminologies, can be further enumerated. However, for a start, a logical composition of terminologies would be the core characteristics of a typical cloud service such as on-demand self-service, broad network access, resource pooling, measured services, mode of payment of service, elastic IP address, and storage volume. However, an assumption can be deduced to generalize the terminologies at the high-level. The next phase of the lifecycle covers the process of developing competency questions. Competency question is a list of questions which

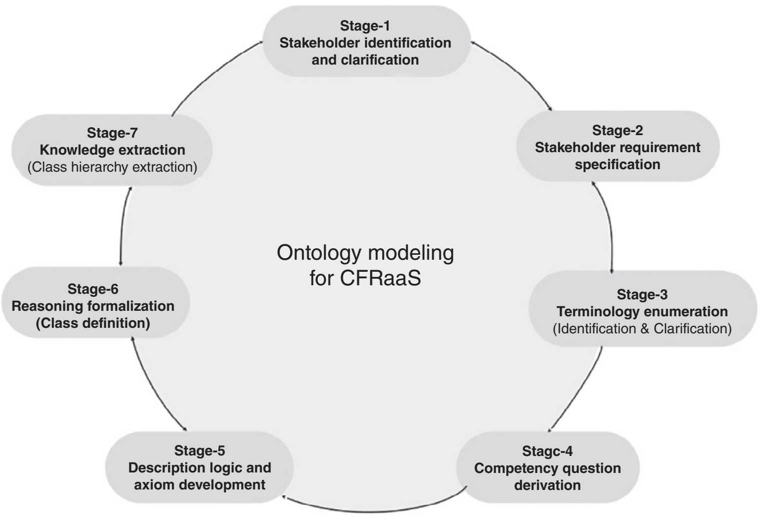
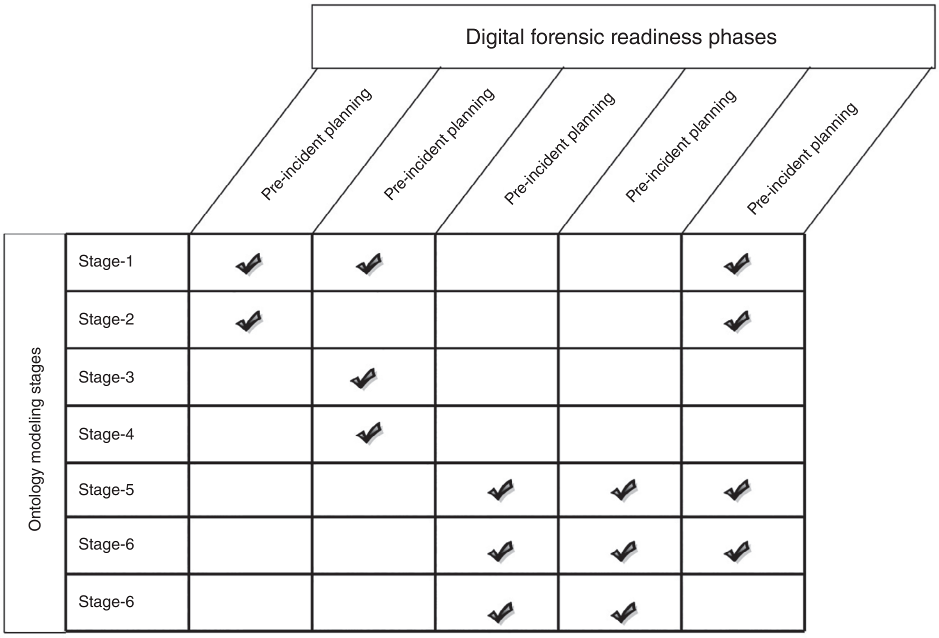


FIGURE 5 CFRaaS ontology development lifecycle. CFRaaS, Cloud Forensic Readiness as a Service

presents metrics for measuring the effectiveness of the knowledge base. It typically helps to answer questions that pertain to the knowledge to be managed. The next phase of the lifecycle involves the development of axioms and description logic. This phase presents a formalization process to the identified terminology, stakeholder requirements, and the logical inter-relation between different terminology and requirement specification. As explained in a recent ontology development process (Ellison et al., 2019), axiom and description logic provide a formalization on which computational process can be carried out. Given such logic, therefore, the high-level structure of CFRaaS can be decomposed into computer reasonable language. Reasoning built on such axiom and logic provides a baseline for CFRaaS domain formalization. Last, knowledge extraction and presentation constitute a milestone in the lifecycle. Given that the development lifecycle expounded in Figure 5 is based on the iterative process, the logical sequence of development is largely context-based. Moreover, the ontology model is applicable to the various layers of the decomposed CFRaaS layer-dependency framework presented in Figure 2. These layers can be, further, mapped into the following DFR phases as illustrated in Figure 6.

6.3.1 | Pre-incident planning

This entails processes that are carried out during cloud platform set-up. Pre-incident planning can, therefore, be described as a process that involves collaboration from all stakeholders. This further implies that pre-incident planning can be integrated at the cloud-platform conceptualization. The pre-incident planning stage of the DFRP cuts across all the layers of the decomposed framework in Figure 2: the service provider layer, virtualization layer, DFR layer, the IRP layer as well as the concurrent processes layer. Therefore, developing an ontology that can integrate all stakeholders in this pre-incident planning can provide a fundamental baseline for effective evaluation of the proposed ontology-driven approach to CFRaaS. By applying the modeling lifecycle presented in Figure 5 to the pre-incident planning stage, an explicit formalization of stakeholder requirements can be derived and measured. For example, the competency question developed for CSP stakeholder can be used to define what the CSP would need to do, to ensure effective CFRaaS implementation. This, in turn, will require input from forensic investigators who will present the essentials required for evidence corroboration. Consequently, the requirement of other stakeholders will be integrated. While this could be an iterative process, the onus of process termination lies with the respective stakeholders.



		Digital forensic readiness phases				
		Pre-incident planning	Pre-incident planning	Pre-incident planning	Pre-incident planning	Pre-incident planning
Ontology modeling stages	Stage-1	✓	✓			✓
	Stage-2	✓				✓
	Stage-3		✓			
	Stage-4		✓			
	Stage-5			✓	✓	✓
	Stage-6			✓	✓	✓
	Stage-6			✓	✓	

FIGURE 6 Mapping of the proposed CFRaaS ontology to ISO/IEC 27043 Standard. CFRaaS, Cloud Forensic Readiness as a Service

6.3.2 | Incident identification phase

Incident identification involves the process of shifting through running processes in the cloud virtualization instances and ascertaining the degree of relevance with respect to a given context. Therefore, the incident identification phase comprises of the development of context-based incident definition, enumeration of different composition (of incidents that can potentially lead to a threat to information security services, as well as the process of ascertaining the probability of incident occurrence). This phase could potentially be defined as the substratum for the DFR process in the cloud platform. Therefore, the application of the ontology development lifecycle in the identification of potential threat instances can provide a collaborative baseline for all stakeholders in the CFRaaS knowledge domain. This can be instrumental to the development of a formalized approach to the implementation of potential cloud-threat instance identification, and definition; a component that has eluded the various stakeholder till now.

6.3.3 | Incident detection phase

Incident detection in a typical cloud platform is dependent on the degree of accuracy of the incident identification phase, to prevent high error rate: false positives and false negatives. However, the context of an incident in the cloud-platform can have a significant impact on the corresponding accuracy of incident identification. Consequently, potential incident detection will require the collaboration of various stakeholders toward the definition of context of an incident, prior to the logic of detection. This further presupposes that context could be fluid, thus eroding the probability of common detection criteria. However, the application of the development lifecycle can be used by the different stakeholders to provide measurable assertions. For instance, a well-developed competency question can provide an explicit marker for incident detection, as what constitutes a threat (for instance) could have been defined.

6.3.4 | Incident preliminary analysis phase

Collaboration among the various stakeholders is a major in this phase. The preliminary analysis can involve an attempt to explore the known and emerging behavioral signature of incidents that can violate information security services. This phase usually involves an iterative process between behavioral analysis and incident detection. By applying the ontology development lifecycle to this phase, various stakeholders can have an explicit description of what constitutes incidents, what to extract from a given incident, what are the dependencies in the different attributes of the running instances in the cloud. Competency questions and requirement specification from different stakeholders can be used to elicit knowledge which can provide explicit formalization process. This is also essential in addressing storage limitations in classical DFR frameworks.

6.3.5 | Readiness formalization phase

by taking input from the preceding phases, the readiness formalization phase integrates output for the CFRaaS. The readiness formalization phase depicts the explicit definition of what constitutes an incident, which entity can be defined as stakeholders for the given context.

7 | COMPARING ONTOLOGY-DRIVEN CFRaaS WITH OTHER EXISTING ONTOLOGY-BASED FORENSIC MODELS

In this section, the authors briefly present a comparative analysis of the ontology-driven CFRaaS with other ontology-driven forensic models that are related or close match to the proposition in the current study. This comparison has mainly been done on the basis of proactiveness (as asserted in the ISO/IEC 27043:2015), incident response capabilities, actual number of phases and key ontology related aspect and challenges in each proposition. Each of the respective literature is also highlighted as shown in Table 2. The motivation behind using proactiveness as a baseline has been necessitated by the fact that CFRaaS is originally a proactive model, and there is a need to maximize the process of

TABLE 2 Comparing ontology-driven CFRaaS with other existing ontology models

Ontology-based models	Proactive forensic approaches	Incident response	No. of phases	Key ontology related aspect	Challenges
Ontology-CFRaaS existing models	Readiness phase (based on ISO/IEC 27043:2015	Incident response procedures (IRP)	5	Semantic matching (terminal classification)	—
1 Ontology model (Semantic web for Digital investigation) (Wimmer, Chen, & Narock, 2018)	—	Graphical user Interface (GUI) for digital investigation tool	Three phases based on (feature selection, registry analyzer, archive, rebuilding, and resolution)	Ontology design patterns for the development of digital forensic tools	Lacks a proactive approach
2 Ontology for IT security Incidents (Wolf, 2013)	—	Investigation of security incidents	—	Ontology for forensic analysis (draws conclusion about the correlation of single results)	Lacks a proactive approach
3 Ontology for reconstruction and analysis of digital incident timelines, ORD21 (Chabot, Bertaux, Nicolle, & Kechadi, 2015)	Extraction layer	Event correlation timeline summarizes illegal active detection	5	An ontology that represents an accurate digital incident that is associated with a digital investigation (associated with a set of tools)	—
4 Ontology framework for Automation (Luthfi, 2014)	—	Acquisition of digital evidence to perform a digital investigation	2	Search against steps in accordance with the rules of ontology	Lacks proactive approaches
5 Investigation through semantic technologies (Amato, Cozzolino, Mazzeo, & Mazzocca, 2017)	Data collection	Correlation of present information acquired from forensic data	5	Approach to conduct a digital investigation based on semantic web technologies (reasoning & rule evaluation)	—
6 DIALOG (Kahvedžić & Kechadi, 2009)	—	Manage, reuse and analysis of digital investigation knowledge	—	Knowledge encapsulation with digital forensics (case of independent vocabulary)	No distinct phases and no proactive approaches
7 Ontology for Digital Security and digital forensic investigative techniques (Ellison & Venter, 2016)	Based on ISO/IEC 27043:2015 guidelines (Readiness, implementation, and Evaluation	Based on ISO/IEC 27043:2015 guidelines (Initialization, acquisitive and investigative	4	Using ontologies to model the domain of technique with digital forensic and security	—
8 Semantic modeling of digital forensic evidence (Kahvedžić & Kechadi, 2010)	—	Evidence management	—	Modeling structure of the vocabulary of terms (to encode the semantic information of evidence)	Lacks a proactive approach and systematic phases of activities

Abbreviation: CFRaaS, Cloud Forensic Readiness as a Service.

conducting digital investigation while minimizing the cost of incident response (Rowlingson, 2004). furthermore, incident response capabilities have been explored to show the need for a post-event response whenever a potential security incident is detected. Logically, the numbers of phases in a given model highlights the sequence and likely composition of such a model. This logic therefore necessitated the inclusion of the number of phases of a model. Therefore, this study asserts that the number of phases can be used to show the systematic iterations/activities when conducting DFIs. It is, however, important to note that the number of phases does not wholly reflect the suitability of the model to digital investigation. However, it has advertently been used to show systematically, how forensic activities transverses within each digital forensic approach. One aspect of the existing works that relates to the proposed ontology-driven CFRaaS is the possible linkage to ontology. Thus, the inclusion of the key ontology related aspect, as a metrics for benchmarking, is essentially required. The key ontology aspects have been discussed to show the role that it can play in a DF ontology modeling process. Last, challenges have been explored to show the key limitation that the existing approaches may have relative to the proposed ontology-driven CFRaaS. The challenges that have been identified have been summed up to come with key contextual evaluations of this research article.

By taking the CFRaaS model as a basis for discussion in this context, it mainly addresses the readiness phases as a proactive phase while the IRP phase as a post incident response phase. Coupled with the introduction of ontology techniques, the proposed approach utilizes semantic matching of cloud forensic terminology for classification. The authors therefore applied this approach as a baseline for this study. Additionally, the authors highlight several propositions put across by existing works on identifying some contributions that can constitute the CFRaaS. For example, an ontology model for the semantic web for digital investigations has an incidence response techniques that integrates graphical user interface to conduct digital investigation processes, with three phases for feature selection, registry analysis, archiving, building, and resolution (Wimmer et al., 2018). The model eventually developed an ontology design pattern useful for the development of a forensic tool. However, it failed in proactivity, which typifies the cloud platform. Hence, the proactive approach presented in ontology-driven CFRaaS constitutes a major distinction from such study. Next, an ontology for IT security void of proactive processes was used to address the incident response process of investigating security incidents. The study used ontology for forensic analysis to draw conclusions about the correlation of a single result (Wolf, 2013). In addition, the study does not have distinct phases that show systematic transition of activities. In a similar approach, an ontology for the reconstruction and analysis of digital incident timelines, was developed by Chabot, Bertaux, Nicolle, and Kechadi (2015). It has an extraction layer as a proactive approach and addresses incident response based on event correlation, and timeline summarization of illegal active detection. With five phases, the study uses ontology approach to represents an accurate digital incident that is associated with a digital investigation and the corresponding set of tools, as summarized in Table 2. The findings in Luthfi (2014) is presented next. Luthfi (2014) developed a two-step ontology framework for automating DFI. The result was asserted to address the challenge of acquisition of digital evidence. To accomplish this, the study uses an ontology technique that searches evidence against investigative steps and in accordance with the rules of ontology. Another proposition (Amato et al., 2017) explores the use of semantic technologies that have employed data collection and correlation of present information from acquired forensic data. This approach uses semantic web technology, reasoning, and rule evaluation to achieve forensic techniques. Next, the DIALOG framework (Kahvedžić & Kechadi, 2009) uses knowledge encapsulation of independent vocabulary with digital forensic cases. This framework addresses incidence response by highlighting management, reusability, analysis of digital investigation knowledge. Next, research on ontology for digital security and forensics (Ellison & Venter, 2016) uses an ontology to model domains of techniques within DF and security. The study attempted to address proactiveness (Readiness implementation and evaluation) and reactiveness (initialization, acquisitive and investigative) based on the guidelines mentioned in ISO/IEC 27043:2015. An improved version of similar ontology model is further presented in Ellison et al. (2017). Other research includes semantic modeling of digital forensic evidence by (Kahvedžić & Kechadi, 2010), which attempt to model the structured vocabulary of terms by encoding the semantic information of evidence, by addressing evidence management in incident response. However, this study does not have a distinct number of phases neither does it address proactive approaches.

8 | DISCUSSION AND EVALUATION OF THE PROPOSITIONS

The huge and complex amount of digital forensic data that is collected by CFRaaS in order to forensically prepare the cloud for digital investigations need to be synthesized, so that it can be easy for digital forensic investigators, to be able to interpret what that digital data represents and the semantics that is involved. In order to fulfill this process, Section 6

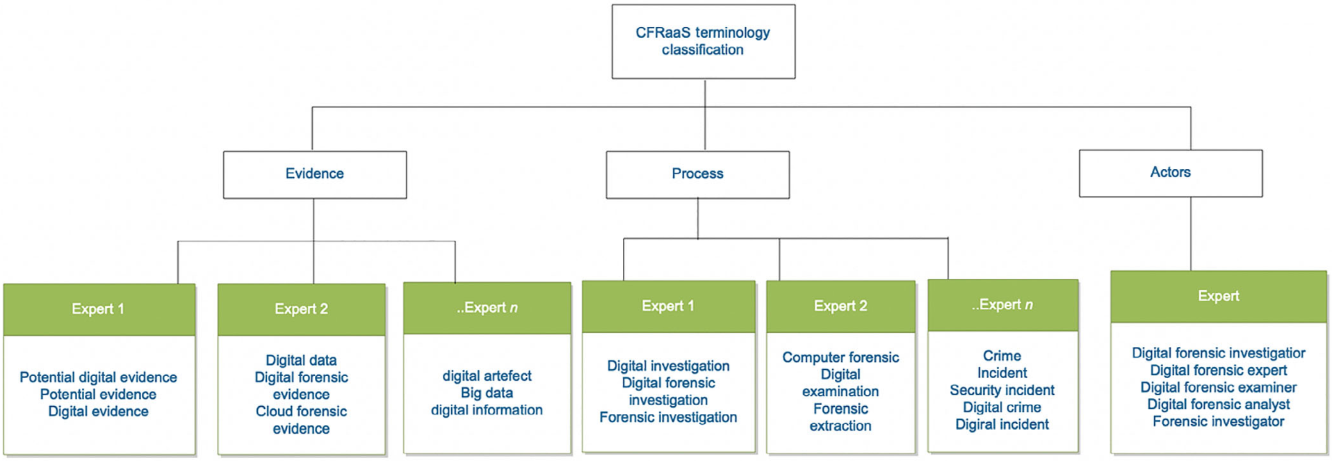


FIGURE 7 Classification of CFRaaS terminologies disparities. CFRaaS, Cloud Forensic Readiness as a Service

highlighted steps (Sections 6.3.1–6.3.5) based on the layer dependencies and approaches that may be used to build a forensic readiness ontology in the cloud, precisely for CFRaaS. Basically, this approach is aimed at presenting the concept and relationships that may be used to show the relevance that exists between digital crime scenes, the process used to commit the crime, tools used, and the investigative processes that could be leveraged. A more promising prospect that has aided in setting the precedence toward building ontology-driven CFRaaS has been through the presentation of a formal approach of layer dependencies. The layer dependencies make it possible for stakeholders to be able to extract forensic knowledge that can be used by DFIs, particularly during artifact filtering. This can be achieved through the mapping of processes as Sets and subprocesses as Subsets. Such a relationship, for instance, has been explicitly highlighted. Generally, generating reasoning or knowledge base from a plethora of digital data may be a time consuming and tedious process. Extracting such knowledge base can be further hindered if there exist complexities in the mining process of useful knowledge and it is on this basis, that the authors have arrived at these propositions.

While it is important to mention that CFRaaS does not collect digital information in a structured format (VM images, VM logs, software logs, window file system), one would need to carefully analyze this so that information that contains incidents are not missed. Consequently, a CFRaaS ontology would carefully highlight or provide semantic matching and reasoning approaches that would carefully cluster different incidental digital artifacts. Also, if the modeled CFRaaS ontology lacks semantic matching techniques that could be used to provide reasoning, then it may defeat the purpose that CFRaaS is expected to achieve. In view of the foregoing, it is worthy to mention that the CFRaaS ontology that has been suggested in this article structures knowledge based on the CFRaaS processes and subprocess. By integrating this approach, a synergistic relationship between each of the processes can be harnessed. This process typically constitutes the classical process of a knowledge base. These dependencies can help forensic investigators (and other applicable stakeholders) to be able to build relationships and or taxonomies between digital data and interaction constraints. Grober (1993) has highlighted that reliable knowledge during a digital investigation could be represented by an ontology. Based on this, the ontology lifecycle that is shown in Section 6.3 should follow some rules in order to alleviate disparities that may exist. Also, while the focus of the CFRaaS is to achieve a forensic strategy in the cloud environment, it is also important to highlight the knowledge base that a digital forensic investigator may need in order to accomplish an investigative task in a complex setting or in an open cloud environment. An ontology-driven CFRaaS achieve this, for instance, by conducting terminology enumeration which can be used to develop a forensic knowledge base. This approach can help the digital forensic investigators and the LEAs stakeholders to resolve disparities that could exist between terminologies as highlighted in Section 6.3. Forensic experts may interpret the different sets of relevant terminologies based on evidence, process, and actors as shown in Figure 7. This further illustrates the potential disparities in cloud/digital forensic terminologies that may exist when ontologies are not employed in a CFRaaS.

Figure 7 shows different cloud/digital forensic terminologies that may result in semantic conflicts if they are not modeled from an ontological perspective. Based on this classification, it is important to say that a DFE [Expert 1] may interpret [Evidence] as {*Potential digital evidence*}, or as {*potential evidence*} or as {*digital evidence*} while another [Expert 2] may interpret the same evidence as {*digital data*} ≈ {*digital forensic evidence*} ≈ {*cloud forensic evidence*} respectively. Notably [Expert *n*] may interpret the same evidence as {*digital artifact*} ≈ {*big data*} ≈ {*digital information*}. More so, the investigative process may also be viewed differently with different experts. For example, [expert 1] may interpret it as {*digital investigation*} ≈ {*digital forensic investigation*} and {*forensic investigation*} while [Expert 2] may interpret it as {*computer forensic*} ≈ {*digital examination*} *and* {*forensic extraction*}. [Expert n] may interpret {*crime*} ≈ {*incident*} ≈ {*security incident*} ≈ {*digital crime*} ≈ {*digital incident*} to have the same relevance. Next, the CFRaaS [actors], may be interpreted as follows: {*Digital forensic investigators*} ≈ {*digital forensic experts*} ≈ {*digital forensic examiner*} ≈ {*digital forensic analyst*} and {*forensic investigator*}.

While the CFRaaS ontology formulation steps in Figure 5 show a recurring process, the study has chosen the terminology disparities to show how the absence of proper interpretation may lead either to redundancy in investigation or challenges during an investigation, litigation, or evidence presentation either through reporting or forensic interpretation (Karie, Kebande, Venter, & Choo, 2019).

The view of the terminologies disparities is one among many reasons that show the need for modeling CFRaaS ontologies in order to be able to create strong and dynamic digital forensic platform that can be able to help investigators in different aspects. In order to be able to develop a competency-based ontological approach, the authors suggest that a well-modeled ontology should be able to put across logic descriptions and formal reasoning in order to ease the digital investigative processes and to extract knowledge that can assist in digital investigation, particularly, in a timely and effective manner.

It is indispensable to highlight that an organization that employs forensic readiness can minimize the effort that is needed to conduct a DFI if a security incident is detected during incident response. This study posits that, based on the CFRaaS flow-processes (layer dependencies) and the objectives that CFRaaS is meant to achieve, it should coexist in an environment with regulatory compliance, a forensic strategy, acceptable forensic technologies with more realistic forensic policies in order for the aforementioned propositions to be effectively achieved. While forensic readiness may be viewed as an optional approach for some organizations, the digital investigation approach may be costlier than implementing forensic readiness. That notwithstanding, conducting a DFI in the cloud environment faces several technical, operation, and jurisdictional issues. However, based on the nature of CFRaaS and its realistic readiness approaches that conform to ISO/IEC 27043 international standards, it is best suited to model using proactive ontology (Kebande & Venter, 2015). This assumes that the cloud infrastructures and its functionalities remain untampered with or altered during the forensic readiness processes. Nevertheless, given that the cloud is advertently a security threat to forensic artifacts, it supports logic to develop an ontology-driven approach that can provide reasoning as well as knowledge extraction from the cloud environment. This can be used to address long-term issues of the cloud environment, through the careful removal of what is deemed as evidence while ensuring the sanctity of the same evidence is upheld.

BOX 1 Cyber threat-intelligence perspective of ontology-driven CFRaaS

The technique of using ontologies for modeling CFRaaS presents a lightweight approach that can leverage the novel approaches that have been embedded in CFRaaS; an approach that transforms the dangerous-information collecting botnets to a software forensic agents that can aid in achieving forensic readiness in the cloud environment. The need to extract shared knowledge or intelligence from cloud infrastructures is a step toward a steady detection and prevention of potential security incidents from the perspective of DF. The current threat intelligence perspective that is based on the modeled CFRaaS could easily be achieved through intelligence and vulnerability repositories from different jurisdictions (Karie et al., 2019). This ends up being useful to organizations and it becomes paramount to extract threats or information about vulnerabilities in real-time and when needed.

9 | CONCLUSION AND FUTURE WORK

The current trends in cyber-security show that the dynamics of cybercrime are changing due to the complexity of adversaries and the increase in volumes of data as a result of the increase in digital devices. Nevertheless, there has been a change in the approaches used in identifying, collecting, storing, analyzing, and even presenting digital data that may be used during litigation. In this article, the authors have mainly focused on developing approaches that can be used to combat the issues that exist in a cloud environment. This is achieved through the integration of the CFRaaS with ontologies in order to address the constraints that may hinder forensic tools from achieving investigative objects in a timely and effective manner. The study argued that the process of employing ontologies to CFRaaS could help in the creation of a strong digital investigation platform that may address future challenges with a degree of certainty. Furthermore, the study has been able to identify techniques of presenting an ontology-driven CFRaaS based on the CFRaaS layer dependencies and this contribution formed the main discussion of this article. As part of future work, the authors aim to engage the views and reviews of experts in order to identify relevant opinions that can help to evaluate this study.

ACKNOWLEDGMENTS

The authors wish to thank Department of Computer Science, Malmö Universitet, Sweden, Security Research Institute, Edith Cowan University, Australia, Cyber Security and Networking Department, Qatar Community College, Qatar and DigiFORs Research group, Department of Computer Science, University of Pretoria, South Africa for the support toward coming up with this research. The authors acknowledge that opinions, findings and conclusions or recommendations expressed in this publication are purely those of the authors.

CONFLICT OF INTEREST

The authors have declared no conflicts of interest for this article.

AUTHOR CONTRIBUTIONS

Nickson Karie: Conceptualization; writing-original draft. **Richard Adeyemi:** Formal analysis; investigation; writing-review and editing. **H. S. Venter:** Supervision.

ORCID

Victor R. Kebande https://orcid.org/0000-0003-4071-4596
Nickson M. Karie https://orcid.org/0000-0001-5173-9268
Richard A. Ikuesan https://orcid.org/0000-0001-7355-2314
Hein S. Venter https://orcid.org/0000-0002-3607-8630

FURTHER READING

Singh, A., Ikuesan, A. R., & Venter, H. S. (2018, September). Digital forensic readiness framework for ransomware investigation. In *International conference on digital forensics and cyber crime* (pp. 91–105). Cham, Switzerland: Springer.

Kebande, V. R. (2018). *A novel cloud forensic readiness service model*. (Doctoral dissertation). University of Pretoria, Pretoria).

Kebande, V. R., & Venter, H. S. (2018). Novel digital forensic readiness technique in the cloud environment. *Australian Journal of Forensic Sciences*, *50*(5), 552–591.

Venter, H. S., Karie, N. M., & Kebande, V. R. (2017). *Taxonomy for digital forensic evidence*. Nairobi: IEEE.

Kebande, V. R., & Venter, H. S. (2018). On digital forensic readiness in the cloud using a distributed agent-based solution: Issues and challenges. *Australian Journal of Forensic Sciences*, *50*(2), 209–238.

Kebande, V. R., & Venter, H. S. (2016). Requirements for achieving digital forensic readiness in the cloud environment using an NMB solution. In *11th International Conference on Cyber Warfare and Security: ICCWS* (p. 399).

Kebande, V., Ntsamo, H. S., & Venter, H. S. (2016, July). Toward a prototype for achieving digital forensic readiness in the cloud using a distributed NMB solution. In *European Conference on Cyber Warfare and Security* (p. 369). Academic conferences international limited.

REFERENCES

Amato, F., Cozzolino, G., Mazzeo, A., & Mazzocca, N. (2017). Correlation of digital evidences in forensic investigation through semantic technologies. In *2017 31st International Conference on advanced information networking and applications workshops (WAINA)* (pp. 668–673). Taipei, Taiwan: IEEE.

Alruban, A., Clarke, N., Li, F., & Furnell, S. (2017). Insider misuse attribution using biometrics. In *ARES '17: Proceedings of the 12th International Conference on Availability, Reliability and Security, (September)* (pp. 1–7). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3098954.3103160

Brinson, A., Robinson, A., & Rogers, M. (2006). A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Digital Investigation*, *3*, 37–43.

Chabot, Y., Bertaux, A., Nicolle, C., & Kechadi, T. (2015). An ontology-based approach for the reconstruction and analysis of digital incidents timelines. *Digital Investigation*, *15*, 83–100.

Delport, W., Köhn, M., & Olivier, M. S. (2011, August). Isolating a cloud instance for a digital forensic investigation. In *Information Security of South Africa, (ISSA)*. IEEE.

Delugach, H. S., Cox, L. C., & Skipper, D. J. (2016). Representing software component dependencies using conceptual graphs. https://pdfs.semanticscholar.org/d1f4/d1ca944232806fd002f8fd972079e04dca22.pdf

Ellison, D., & Venter, H. (2016). An ontology for digital security and digital forensics investigative techniques. In *Proceedings of the 11th international conference on cyber warfare and security, ICCWS* (pp. 119–127). Munich, Germany.

Ellison, D., Ikuesan, A. R., & Venter, H. (2019). Description logics and axiom formation for a digital forensics ontology. In *European Conference on Cyber Warfare and Security* (pp. 742–XIII). Academic Conferences International Limited.

Ellison, D., Venter, H., & Ikuesan, A. (2017). An improved ontology for knowledge management in security and digital forensics. In *European Conference on Cyber Warfare and Security* (pp. 725–733). Academic Conferences International Limited.

Ikuesan, A. R., & Venter, H. S. (2017). Digital forensic readiness framework based on behavioral-biometrics for user attribution. In *2017 IEEE Conference on Applications, Information and Network Security, AINS 2017* (pp. 54–59), *1 January* 1. https://doi.org/10.1109/AINS.2017.8270424

Ikuesan, A. R., & Venter, H. S. (2019). Digital behavioral-fingerprint for user attribution in digital forensics: Are we there yet? *Digital Investigation*, *30*, 73–89. https://doi.org/10.1016/j.diin.2019.07.003

Karie, N. M., Kebande, V. R., Venter, H. S., & Choo, K. K. R. (2019). On the importance of standardising the process of generating digital forensic reports. *Forensic Science International: Reports*, *1*, 100008.

Kebande, V. R., & Venter, H. S. (2015). Adding event reconstruction to a Cloud Forensic Readiness model. In *2015 Information Security for South Africa (ISSA)* (pp. 1–9). IEEE.

Kebande, V. R., & Venter, H. S. (2014). A cloud forensic readiness model using a Botnet as a Service. In *The international conference on digital security and forensics (DigitalSec2014)* (pp. 23–32). Ostrava: The Society of Digital Information and Wireless Communication.

Kebande, V. R., & Venter, H. S. (2019). A comparative analysis of digital forensic readiness models using CFRaaS as a baseline. *Wiley Interdisciplinary Reviews: Forensic Science*, *1*, e1350.

Karie, N. M., & Venter, H. S. (2014). Toward a general ontology for digital forensic disciplines. *Journal of Forensic Sciences*, *59*(5), 1231–1241.

Karie, N. M., & Kebande, V. R. (2016). Building ontologies for digital forensic terminologies. *International Journal of Cyber-Security and Digital Forensics*, *5*(2), 75–83.

Kahvedžić, D., & Kechadi, T. (2009). DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge. *Digital Investigation*, *6*(supplement), S23–S33.

Kahvedžić, D., & Kechadi, T. (2010). Semantic modelling of digital forensic evidence. In *International Conference on Digital Forensics and Cyber Crime* (pp. 149–156). Berlin, Heidelberg: Springer.

Karie, N. M., & Kebande, V. R. (2018). Knowledge management as a strategic asset in digital forensic investigations. *International Journal of Cyber-Security and Digital Forensics*, *7*(1), 10–20. https://doi.org/10.17781/p002311

Luthfi, A. (2014). The use of ontology framework for automation digital forensics investigation. *International Journal of Computer, Control, Quantum and Information Engineering*, *8*(3), 423–425.

McGuinness, D. L., & Noy, N. F. (2000). *Ontology Development 101: A guide to creating your ontology* (pp. 1–25). Retrieved from http://protege.stanford.edu/publications/ontology_development/ontology101.pdf

Park, H., Cho, S., & Kwon, H. C. (2009, January). Cyber forensics ontology for cyber criminal investigation. In *International Conference on Forensics in Telecommunications, Information, and Multimedia* (pp. 160–165). Springer, Berlin, Heidelberg. Retrieved from http://protege.stanford.edu/publications/ontology_development/ontology101.pdf

Rowlingson, R. (2004). A ten-step process for forensic readiness. *International Journal of Digital Evidence*, *2*(3), 1–28.

Raad, J., & Cruz, C. (2015). A survey on ontology evaluation methods. In *IC3K 2015 - Proceedings of the 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management* (Vol. 2, pp. 179–186). https://doi.org/10.5220/0005591001790186

Slay, J., & Schulz, F. (2014). Development of an ontology based forensic search mechanism: Proof of concept. *arXiv preprint arXiv:1407.8258*.

Valjarevic, A., & Venter, H. S. (2015). Introduction of concurrent processes into the digital forensic investigation process. *Australian Journal of Forensic Sciences*, *48*(3), 1–19.

Wimmer, H., Chen, L., & Narock, T. (2018). Ontologies and the semantic web for digital investigation tool selection. *Journal of Digital Forensics, Security and Law*, *13*(3), 6.

Wolf, J. P. (2013). *An ontology for digital forensics in IT security incidents*. Augsburg, Germany: University of Augsburg.

How to cite this article: Kebande VR, Karie NM, Ikuesan RA, Venter HS. Ontology-driven perspective of CFRaaS. *WIREs Forensic Sci*. 2020;2:e1372. https://doi.org/10.1002/wfs2.1372