Towards the Representation of Network Assets in Health Care Environments Using Ontologies

Lucía Prieto Santamaría[1,2] David Fernández Lobón[2] Antonio Jesús Díaz-Honrubia[1,2]
Ernestina Menasalvas Ruiz[1,2] Sokratis Nifakos[3] Alejandro Rodríguez-González[1,2]

[1] ETS Ingenieros Informáticos, Universidad Politécnica de Madrid, Madrid, Spain
[2] Centro de Tecnología Biomédica, Universidad Politécnica de Madrid, Madrid, Spain
[3] Department of Learning, Informatics, Management and Ethics, Karolinska Institute, Stockholm, Sweden

Address for correspondence Lucía Prieto Santamaría, MSc, Centro de Tecnología Biomédica, Parque Científico y Tecnológico de la Universidad Politécnica de Madrid, Crta. M40, Km. 38, 28223 Pozuelo de Alarcón, Madrid, Spain (e-mail: lucia.prieto.santamaria@upm.es).

Methods Inf Med 2021;60:e89–e102.

Abstract

Objectives The aim of the study is to design an ontology model for the representation of assets and its features in distributed health care environments. Allow the interchange of information about these assets through the use of specific vocabularies based on the use of ontologies.

Methods Ontologies are a formal way to represent knowledge by means of triples composed of a subject, a predicate, and an object. Given the sensitivity of network assets in health care institutions, this work by using an ontology-based representation of information complies with the FAIR principles. Federated queries to the ontology systems, allow users to obtain data from multiple sources (i.e., several hospitals belonging to the same public body). Therefore, this representation makes it possible for network administrators in health care institutions to have a clear understanding of possible threats that may emerge in the network.

Results As a result of this work, the "Software Defined Networking Description Language—CUREX Asset Discovery Tool Ontology" (SDNDL-CAO) has been developed. This ontology uses the main concepts in network assets to represent the knowledge extracted from the distributed health care environments: interface, device, port, service, etc.

Conclusion The developed SDNDL-CAO ontology allows to represent the aforementioned knowledge about the distributed health care environments. Network administrators of these institutions will benefit as they will be able to monitor emerging threats in real-time, something critical when managing personal medical information.

Keywords
- network assets
- ontologies
- health care cybersecurity
- knowledge representation

received
April 14, 2021
accepted after revision
July 20, 2021
published online
October 5, 2021

DOI https://doi.org/10.1055/s-0041-1735621.
ISSN 0026-1270.

Georg Thieme Verlag KG, Rüdigerstraße 14, 70469 Stuttgart, Germany

Introduction

Over the past 20 years, the integration of new technology in health care has significantly changed. Hospitals, clinics as well as health care research institutes rely on computer-based infrastructures, and they become more connected over network and cloud technologies. Moreover, new set of medical devices and health applications have been integrated within health care services, upgrading the interaction between patients and clinicians and providing additional information (personal health records) which are enhancing the current electronic health records. In addition, the health care sector depends heavily on the safe and reliable operation of its supply chains for the delivery of materials and health information and for enabling patients to receive high quality care in an effective and timely manner.

The health care supply chain includes among others, manufacturers (medical equipment, and hospital medical suppliers), distributors, medical service providers, medical groups, insurance companies, government agencies, employers, government regulators, patients, and other users of health care services operating in a complex and highly interconnected environment. This is increasingly a data-driven ecosystem populated by connected devices (often Internet-connected), shared medical databases and networks, and it is precisely this interconnected nature and the high criticality of the sector that make it a prime target for cyberattacks.

The transformation of the conventional health care systems and services to a secure smart ecosystem is under investigation by several researchers. Cybersecurity tools, policies, and frameworks are required, to increase patients' safety as well as to protect their medical data effectively. By integrating efficient security management, risk assessment and data privacy protection frameworks and tools at the core of the systems' design, the health care organizations, such as hospitals, clinics, and research institutes will be able to deliver safe services.

Within Computer Science a "system" is characterized as: "*the collection of multiple entities such as devices (mobile phones, sensors) software (operating systems, development platforms, programs, apps), companies (device manufacturers, carrier, app stores), processes (networking, Short Message Service - SMS, database transactions), and end users/stakeholders (patients, IT managers, health care managers).*"[1] Cybersecurity refers to "the protection of computer-based technology from deliberate or inadvertent disruption via manipulation of underlying software, hardware, or networked connections."[2] There are currently software tools able to collect detailed data about the information and communication technology (ICT) infrastructure, and relate this information with cybersecurity data (vulnerabilities, severity, remediation measures, etc.) made available by international cybersecurity authorities. These tools make use of cybersecurity metrics, standards, protocols, and strategies to identify, understand, and anticipate potential organizational cybersecurity problems.

In this article we are focusing on the health care IT infrastructure which according to ENISA belongs among the critical information infrastructures.[3] The definition of CII taken from the Council Directive 2008/114/EC[4] on the identification and designation of European Critical Infrastructures (ECI) and the assessment of the need to improve their protection establishes that: "*ICT systems are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc.).*" Based on this "in force" directive, organizations within European Union should set up in place "operator security plans (OSPs) or equivalent measures comprising an identification of important assets, a risk assessment and the identification, selection, and prioritization of counter measures and procedures in all designated ECI. It is obvious that in order for organizations to create OSPs, it is important among other issues to be able to share computer network information to better formulate a common identification framework of important assets. For this purpose, interoperability is the most applicable process for allowing distributed systems to communicate. Interoperability processes can develop communication channels between noncommunicable systems, which can be achieved through transforming distributed health care environments data into ontologies.

Thus, in this article we aim to review the current ontologies within computer networks and present a new ontology framework for modeling distributed health care environments data and facilitate semantic interoperability. The manuscript is organized as follows: in the first section, we identify the objectives; in the second section, we include the methods to develop the presented ontology; in the third section, we present the obtained results and discuss them; and finally, in the final section, we state the concluding remarks.

Objectives

- The main objective of the present work is to define an ontology to model distributed health care environments data regarding devices and networks' topologies in the context of detecting security vulnerabilities.
- To review the existing ontologies in the field of computer networks to identify possibilities in reusing for the current proposed model.
- To develop ontological models to represent distributed health care computer networks data by reusing and creating classes and properties consistent with the information context.
- To present a successful use case of the proposed semantic model.

Methods

Distributed Health Care Computer Networks Data

While computer networks have become a key point in modern-day communications, health care environments

demand more complex and elaborated systems to deal with sensitive patient's data. The flow of information and data exchange between the different devices that are involved in these environments can endorse problems at the cybersecurity or privacy levels if specific conditions are not met. It is of utmost importance to well manage and monitor the possible threats that may enclose the communication along such distributed systems to always guarantee those sensitive data privacy and security.

In this context, the H2020-funded CUREX project (https://curex-project.eu/) aims to safeguard patient privacy and increase their trust in currently vulnerable critical health care information infrastructures by analyzing information coming from monitoring data exchanges' risk. For doing this, the first step is to have a detailed inventory of assets. Thus, one of the main parts in the CUREX platform is the Asset Discovery Tool (ADT), which detects all the devices that are connected to a health-related institution network and that may present vulnerabilities compromising the security of the organization's data. The ADT discovers assets (such as health care devices, mobiles, workstations, servers, etc.) connected to the IP network (of a hospital, a health research center, etc.) that can be susceptible to an attack (as operating systems, open ports, etc.), and extracts their related information.

All ADT collected data regarding the overall picture of the network circumstances, must be stored to be further analyzed to detect associated vulnerabilities and to score the cybersecurity and privacy levels of data exchanges. The classical way to structure the information is to store it in a relational database, which can later be queried to examine the possible vulnerabilities of the network. In addition to this relational knowledge base, semantizating the data would provide a meaningful sight to the information that is being gathered. This might help in the subsequent stages to find some vulnerabilities or to detect possible threats by the use of machine learning techniques. Data semantization, defined as "formatting data with reasonable mark-ups and special properties such as tags, labels and many more," overcomes the barriers brought by data heterogeneity and provides possibilities for better understanding of the researched ecosystem.[5]

Within networks' communication and data management research, several solutions have been proposed enabling the access to critical information in health care organizations.[6,7] This research is critical for developing a communication layer between different health care organizations, making it possible to exchange information in a secure and private manner. Moreover, since health care information systems need to be able to communicate complex and detailed medical data securely and efficiently, researchers propose the development of "domain ontologies" for representing network terminology systems.[8–10] On the other hand, one disadvantage of these approaches is that they do not provide solutions that can be applied to different network standards and incoming data. More specifically, what is missing refers to interoperability and transformation frameworks, as a generic approach that will be able to aggregate multiple sets of heterogeneous networking related data, aiming to gain knowledge and offer a greater value to the health care network interoperability.

Among the main objectives of the proposed model in this paper is to provide a structural model that will be able to transform the ingested network datasets into ontologies in terms of structure. We are expecting through this implementation, the upcoming network data to be automatically coordinated and distributed to the corresponding network resources achieving semantic interoperability between health care systems.

Ontologies in Computer Networks

Ontologies are described as formal representations of knowledge that consist of sets of concepts within a particular domain and the relationships established between those concepts. Therefore, they are useful when it comes to express and conceptualize knowledge in a formal and explicitly specified way to share.[11,12] The common method to represent ontologies is by means of triples, following the structure "subject–predicate–object" that can be thought as a graph. Such triples can be stored in multiple manners, being Resource Description Framework (RDF) format[13] as one of the most popular ones.

RDF is a standard model to exchange data in the web. It encompasses a family of specifications developed by the World Wide Web Consortium (W3C), which generates international recommendations and standards that ensure the expansion of the World Wide Web in long terms. The RDF data model is related to SPARQL (SPARQL Protocol and RDF Query Language)[14] queries. Both concepts come under the umbrella of the Semantic Web, which has the main goal of adding semantic and ontological metadata to publish data readable by informatic applications. One of the major advances of this approach would be improving the interoperability, since it would allow data from different sources to be understood and interpreted unambiguously. Nevertheless, data semantization and its representation in ontologies can play an essential role not only in terms of data interoperability, but also in data integration and understanding, giving data consistent unified description formats.

Moreover, RDF allows federated SPARQL queries, in which multiple sources can be queried at the same time. Semantic representation supports the aggregation of data from different sources even if they are not located in the same machine. This represents a big advantage for distributed health care environments as different institutions can merge the information within their own ontologies. In addition, ontologies allow anonymization, since the meaning of the data is given directly by the model in the semantical layer, not by individuals' identification data. For these reasons and in such a context, ontologies provide a great resource to store CUREX data.

It is important to ensure that the semantization is based on FAIR principles,[15] so that the developed ontology

supports the specifications and needs of linked data, providing Findable, Accessible, Interoperable, and Reusable data. This information structure enables the aforementioned flexible and broad queries, being able to link the present data to other databases in just one query. One of the most popular engines to allocate such types of graphs is Virtuoso Server,[16] which allows enabling secure end points to which SPARQL queries and updates can be performed depending on users' grants. This way, the information that has been collected scanning a health institution network can be queried or updated by the corresponding people or applications. The T-Box model, i.e., the terminological component, is usually represented in OWL (Web Ontology Language) format,[17] while the A-Box, i.e., the instances of the model, is typically represented in RDF.

Prior to modelling an appropriate ontology, previous works regarding semantic modelling in the field of computer networks have been revised. One of them, ToCo,[18] is an ontology proposed to represent hybrid telecommunication networks within the framework of the TOUCAN project (Toward Ultimate Convergence of All Networks), describing the physical infrastructure, quality of channel, services, and users in heterogeneous telecommunication networks that span multiple technology domains. A knowledge graph using provenance-aware formalisms for cyber-situational awareness[19] or modeled an ontology-based cybersecurity framework for the Internet of Things has been presented in Mozzaquatro et al.[20] In addition, an OWL-based ontology of information security which modeled assets, threats, vulnerabilities and countermeasures and their relations was also put forward,[21] and ontologies that provided a common, technology independent syntax and semantics for complex communication network concepts were also created.[22]

According to the ADT settings, most parts of the ontology "*Software Defined Networking Description Language*" (SDNDL)[23] would be susceptible to be reused for the current approach. It implements a model that manages the items related to computer networks and their topologies. This ontology, for its part, reuses and is completed with some of the parts from other previous ontologies: the "*Network Description Language*" (NDL),[24] the "*Infrastructure Description Language*" (IDL),[25] and the "*Network Markup Language*" (NML).[26] Hence, given its comprehensiveness and since it covers a great proportion of the elements that the ADT makes use of, SDNDL was chosen to be the main reused resource, as it will be explained in next subsection.

SDNDL-CAO Ontology

SDNDL (Software Defined Networking Description Language)—CAO (CUREX Asset Discovery Tool Ontology) has been developed to give support to devices information data inclusion. The ontology revolves around ADT main concepts: interface, device, port, and service, snapshot, etc. and aims to accommodate diverse information following the semantic web specifications. This way, data can be stored in a Virtuoso Universal Server instance that will be fed up each time a node scans the network system looking for devices (extracting information about the network itself, its topology, and its devices). The main advantage of the current ontology would be that it extends the previous models to provide a semantical data representation model of network topologies regarding devices in the context of security in distributed health care environments.

The ontological model is included in ►Fig. 1, where classes are presented in yellow (those classes with a start superscripted are representing *n-ary* relationships), data properties

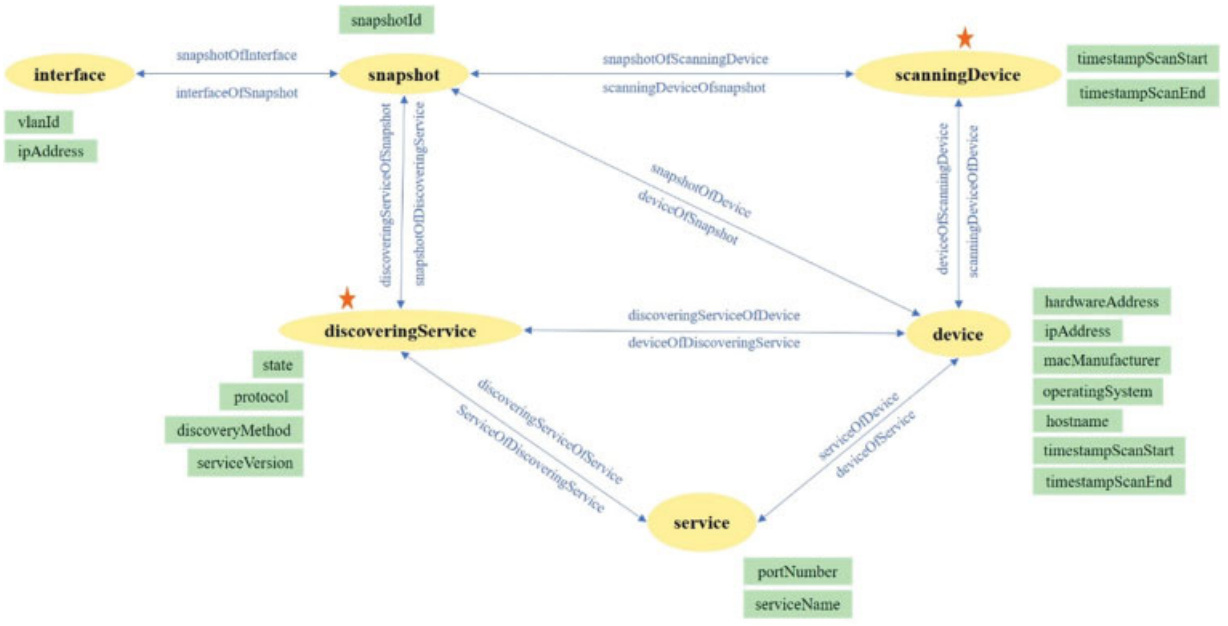

Fig. 1 SDNDL-CAO model. SDNDL-CAO, Software Defined Networking Description Language—CUREX Asset Discovery Tool Ontology.

Table 1 Namespaces used in SDNDL-CAO

Namespace	IRI (Internationalized Resource Identifier)
dc	<http://purl.org/dc/elements/1.1>
ndl-topology-owl	<http://cinegrid.uvalight.nl/owl/ndl-topology.owl>
nml	<http://schemas.ogf.org/nml/2013/05/base>
ns	<http://creativecommons.org/ns>
owl	<http://www.w3.org/2002/07/owl>
rdf	<http://www.w3.org/1999/02/22-rdf-syntax-ns>
rdfs	<http://www.w3.org/2000/01/rdf-schema>
sdndl	<http://www.gsi.dit.upm.es/ontologies/sdndl>
sdndlcao	<http://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao>
xsd	<http://www.w3.org/2001/XMLSchema>

Note: The complete corresponding IRIs for each namespace in the ontology.

are visualized in green, and object properties in blue. The ontology has been developed toward following FAIR principles approach, in English language and under the creative commons license "CC BY 3." Some concepts and terminology have been reused from other ontologies, namely, NLM (http://schemas.ogf.org/nml/2013/05/base), NDL (http://cinegrid.uvalight.nl/owl/ndl-topology.owl), and SDNDL (http://www.gsi.dit.upm.es/ontologies/sdndl). Namespaces used are displayed in the ►**Table 1**. The whole documentation and specifications of SDNDL-CAO is detailed in https://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao/.

Representation of classes (yellow), object properties (blue), and data properties (green) in SDNDL-CAO ontology. Orange stars are placed above classes representing n-ary relationships. Some classes have not been represented for the sake of clarity.

The ontology classes are divided in the actual entities, and in the *n-ary* relationships that have been modeled as classes to store the needed information. Entities are based on the main parts of CUREX ADT: *interface* (a network, a VLAN, that is being scanned to detect devices connected to it), *snapshot* (a configuration of the network while it is being scanned), *device* (asset connected to the network), and *service* (functionality opened in a device that has a port number assigned). The classes that model *n-ary* relationships are two: (1) *scanningDevice* (relationship between a Snapshot and a Device, that has specific timestamps values for the time when the scan started and when it ended), and (2) *discoveringService* (relationship between a *snapshot*, a *device* and a *service*, that has specific values for the service state, service version, the protocol, and the method used for the device discovery).

To implement such classes, we have reused already existing classes from other ontologies, creating new ones only when needed. The classes *networkObject*, *node,* and *service* were imported from NLM; *device*, *interace,* and *networkElement* from NDL; and *snapshot* from SDNDL; while *discoveringService* and *scanningDevice* have been on-purposely created for the current work. The reused classes, although coming from other ontologies, were imported from SDNDL, where these classes were also reused. SDNDL was the main basis for SDNDL-CAO.

Regarding object properties, *deviceOfService* was stated in NLM, and *interfaceOfSnapshot* (originally, *hasSnapshot*) and *snapshotOfInterface* (originally, *isSnapshotOf*) in SDNDL. The rest of object properties used had been specifically created and described in SDNDL-CAO.

Results

The main contribution of the present work is the ontology developed to support the inclusion of distributed health care computer networks' assets vulnerabilities information, called SDNDL-CAO. It is an ontology extended from previous models to incorporate data related to networks management in distributed environments regarding health care and secure systems. SDNDL-CAO has nine different classes described in ►**Table 2**, 16 object properties detailed in ►**Table 3**, and 15 data properties presented in ►**Table 4**.

To illustrate how the triples are stored, semantic data has been generated by scanning a particular network for 24 hours. A total of two snapshots were taken, where eight devices were connected, and 40 different services were identified. One example of an actual named individual is provided in ►**Fig. 2**. This individual is of class *device*, thus having object and data properties that concern such a class. Moreover, ►**Fig. 3** depicts a partial visualization of the class *device* and its named individuals, along with the relationships established between one of such instances and other classes' individuals (in particular, of the class *snapshot*).

Exemplifications of the possibilities when constructing SPARQL queries are included in ►**Figs. 3** to **6**, in which the queries themselves and the returned data are detailed. ►**Figs. 4** and **5** aim to provide more general data, whereas ►**Figs. 6** and **7** serve as use cases of how the graph can be queried depending on specific data needs. In ►**Fig. 4**, information about the VLANs present in the *ADT Triplestore* is retrieved. The output is returned as a table whose columns are the VLAN identifier, the snapshot identifier, and both timestamps of starting and ending the scanning. In ►**Fig. 5**, given a particular snapshot identifier, all the information related to it, is returned. This data is structured in a table that contains information about the VLAN where the snapshot has been taken, about the devices connected and about the open ports and services. ►**Figs. 6** and **7** go further, exploding the benefits of having the knowledge structured in a graph. In ►**Fig. 6**, given a service (for the example we used "mysql"), data about the devices in which the service is open is provided. In ►**Fig. 7**, the user looks for those devices that have been scanned in several snapshots.

Table 2 Description of SDNDL-CAO classes

Class label	Origin	IRI	Comment	Is defined by	Super/subclass
device	ndl-topology	http://cinegrid.uvalight.nl/owl/ndl-topology.owl#Device	"A (collection of) network element(s) that is grouped together representing a physical or abstracted network device. A device may be able to switch on multiple layers. To specifically signify that a device is a physical device, the instance should also be of type PhysicalElement."	http://cinegrid.uvalight.nl/owl/ndl-topology.owl	Superclass: networkElement
discoveringService[a]	sdndl-cao	http://medal.ctb.upm.-es/projects/CUREX/ontologies/sdndlcao#discoveringService	"The ternary relationship between a snapshot, a device and a service. Each time a snapshot is taken, devices are scanned. Each scanned device can have open services. They may have different values for "state," "protocol" and "discoveryMethod" each time a snapshot is taken. Snapshot - Device - Service."	http://medal.ctb.upm.-es/projects/CUREX/ontologies/sdndlcao	–
interface	ndl-topology	http://cinegrid.uvalight.nl/owl/ndl-topology.owl#Interface	"A network (in CUREX - ADT context, a VLAN)."	http://cinegrid.uvalight.nl/owl/ndl-topology.owl	Superclass: networkObject
networkElement	ndl-topology	http://cinegrid.uvalight.nl/owl/ndl-topology.owl#NetworkElement	"A network element. Thus, any object that describes an element in a computer network."	http://cinegrid.uvalight.nl/owl/ndl-topology.owl	Subclass: device
networkObject	nml	http://schemas.ogf.org/nml/2013/05/base#NetworkObject	"A network object. Rather an interface, a node or a service."	http://schemas.ogf.org/nml/2013/05/base	Subclasses: interface, node, service
node	nml	http://schemas.ogf.org/nml/2013/05/base#Node	"Element connected to a network (in CUREX - ADT context, a device)."	http://schemas.ogf.org/nml/2013/05/base	Superclass: networkObject
scanningDevice[a]	sdndl-cao	http://medal.ctb.upm.-es/projects/CUREX/ontologies/sdndlcao#scanningDevice	"The relationship between a snapshot, the device from where the network was scanned and the start and end timestamps when the scanning was carried out. Snapshot - Device (with a Timestamp associated with the relationship)."	http://medal.ctb.upm.-es/projects/CUREX/ontologies/sdndlcao	–
service	nml	http://schemas.ogf.org/nml/2013/05/base#Service	"An open service in a device."	http://schemas.ogf.org/nml/2013/05/base	Superclass: networkObject
snapshot	sdndl	http://www.gsi.dit.upm.-es/ontologies/sdndl#Snapshot	"A snapshot taken between start and end timestamps of the configuration of a network and its devices."	http://www.gsi.dit.upm.-es/ontologies/sdndl	–

[a]These classes have been specifically created for the current ontology.

Table 3 Description of SDNDL-CAO object properties

Object property label	Origin	IRI	Comment	Domain	Range	Is inverse of
deviceOfDiscoveringService[a]	sdndl-cao	http://medal.ctb.upm.-es/projects/CUREX/ontologies/sdndlcao#deviceOfdiscoveringService	"Relationship between a device and a discoveringService entity. One device may be associated with multiple discoveringService entities."	device	discoveringService	discoveringServiceOfDevice
deviceOfScanningDevice[a]	sdndl-cao	http://medal.ctb.upm.-es/projects/CUREX/ontologies/sdndlcao#deviceOfScanningDevice	"Relationship between a device and a discoveringService entity. One device may be associated with multiple discoveringService entities."	device	scanningDevice	scanningDeviceOfDevice
deviceOfService	nml	http://schemas.ogf.org/nml/2013/05/base#deviceOfService	"Relationship between a device and an open service. Multiple services may be associated with a device."	device	service	serviceOfDevice
deviceOfSnapshot[a]	sdndl-cao	http://medal.ctb.upm.-es/projects/CUREX/ontologies/sdndlcao#deviceOfSnapshot	"Relationship between a device and a snapshot. A device can be associated with multiple snapshots."	device	snapshot	snapshotOfDevice
discoveringServiceOfDevice[a]	sdndl-cao	http://www.medal.ctb.upm.es/ontologies/sdndlcao#discoveringServiceOfDevice	"Relationship between a discoveringService entity and a device. One discoveringService entity is associated with one device."	discoveringService	device	deviceOfDiscoveringService
discoveringServiceOfService[a]	sdndl-cao	http://www.medal.ctb.upm.es/ontologies/sdndlcao#discoveringServiceOfService	"Relationship between a discoveringService entity and a service. One discoveringService is associated with one service."	discoveringService	service	serviceOfDiscoveringService
discoveringServiceOfSnapshot[a]	sdndl-cao	http://medal.ctb.upm.-es/projects/CUREX/ontologies/sdndlcao#discoveringServiceOfSnapshot	"Relationship between a discoveringService entity and a snapshot. One discoveringService is related to one snapshot."	discoveringService	snapshot	snapshotOfDiscoveringService
interfaceOfSnapshot	sdndl	http://www.gsi.dit.upm.es/ontologies/sdndl#hasSnapshot	"Relationship between a VLAN and a snapshot. A VLAN may have multiple snapshots."	NetworkObject	snapshot	snapshotOfInterface
scanningDeviceOfDevice[a]	sdndl-cao	http://www.medal.ctb.upm.es/ontologies/sdndlcao#scanningDeviceOfDevice	"Relationship between a scanningDevice entity and a device. One scanningDevice is associated with one device."	scanningDevice	device	deviceOfScanningDevice
scanningDeviceOfSnapshot[a]	sdndl-cao	http://www.medal.ctb.upm.es/ontologies/sdndlcao#scanningDeviceOfSnapshot	"Relationship between a scanningDevice entity and a snapshot. One scanningDevice entity is associated with one snapshot."	scanningDevice	snapshot	snapshotOfScanningDevice
serviceOfDevice[a]	sdndl-cao	http://medal.ctb.upm.-es/projects/CUREX/ontologies/sdndlcao#serviceOfDevice	"Relationship between a service and a device. Same service may be open in several devices."	snapshot	device	deviceOfService
serviceOfDiscoveringService[a]	sdndl-cao	http://medal.ctb.upm.-es/projects/CUREX/ontologies/sdndlcao#serviceOfDiscoveringService	"Relationship between a service and a dicoveringService entity. One service may be associated with multiple discoveringService entities."	service	discoveringService	discoveringServiceOfService
snapshotOfDevice[a]	sdndl-cao	http://medal.ctb.upm.-es/projects/CUREX/ontologies/sdndlcao#snapshotOfDevice	"Relationship between a snapshot and a device. There may be multiple devices connected to a taken snapshot of a VLAN."	snapshot	device	deviceOfSnapshot
snapshotOfDiscoveringService[a]	sdndl-cao	http://medal.ctb.upm.-es/projects/CUREX/ontologies/sdndlcao#snapshotOfDiscoveringService	"Relationship between a snapshot and a discoveringService entity. One snapshot may be associated with several discoveringService entities."	snapshot	discoveringService	discoveringServiceOfSnapshot
snapshotOfInterface	sdndl	http://www.gsi.dit.upm.es/ontologies/sdndl#isSnapshotOf	"Relationship between a snapshot and an interface (a VLAN). One snapshot is associated with one VLAN."	snapshot	NetworkObject	interfaceOfSnapshot
snapshotOfScanningDevice[a]	sdndl-cao	http://medal.ctb.upm.-es/projects/CUREX/ontologies/sdndlcao#snapshotOfScanningDevice	"Relationship between a snapshot and a scanningDevice entity. A snapshot is associated with one scanningDevice."	snapshot	ScanningDevice	scanningDeviceOfSnapshot

[a]These object properties have been specifically created for the current ontology.

Table 4 Description of SDNDL-CAO data properties

Data property label	Origin	IRI	Comment	Domain	Range
discoveryMethod[a]	sdndl-cao	http://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#discoveryMethod	"Method used for a specific port and service's discovery."	discoveringService	String
hardwareAddress	sdndl	http://www.gsi.dit.upm.es/ontologies/sdndl#hardwareAdress	"The MAC address of a device."	device	String
Hostname[a]	sdndl-cao	http://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#hostname	"The hostname of the device."	device	String
ipAddress	sdndl	http://www.gsi.dit.upm.es/ontologies/sdndl#ipAdress	"The IP address of a network object (we will consider devices and VLANs IPs)."	networkObject	String
macManufacturer[a]	sdndl-cao	http://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#macManufacturer	"The MAC manufacturer's address of a device."	device	String
operatingSystem[a]	sdndl-cao	http://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#operatingSystem	"The operating system of a device."	device	String
portNumber	sdndl	http://www.gsi.dit.upm.es/ontologies/sdndl#portNumber	"A port number associated with a service."	service	Integer
protocol[a]	sdndl-cao	http://www.medal.ctb.upm.es/ontologies/sdndlcao#protocol	"The transport protocol associated with a port and service (e.g., tcp/ip)."	discoveringService	String
serviceName[a]	sdndl-cao	http://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#serviceName	"The name of a service."	service	String
serviceVersion[a]	sdndl-cao	http://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#serviceVersion	"The version of a service."	discoveringService	String
snapshotId[a]	sdndl-cao	http://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#snapshotId	"The ID of a snapshot."	snapshot	String
state[a]	sdndl-cao	http://www.medal.ctb.upm.es/ontologies/sdndlcao#state	"The state in which a specific port is at a discovery time."	discoveringService	String
timestampScanEnd[a]	sdndl-cao	http://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#timestampScanEnd	"Timestamp referred to the time when the scanning ends."	–	Date time stamp
timestampScanStart[a]	sdndl-cao	http://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#timestampScanStart	"Timestamp referred to the time when the scanning starts."	–	Date time stamp
vlanId[a]	sdndl-cao	http://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#vlanId	"The ID of a VLAN."	interface	String

[a]These data properties have been specifically created for the current ontology.

```
@prefix dc: <http://purl.org/dc/elements/1.1/> .
@prefix ndl-topology-owl: <http://cinegrid.uvalight.nl/owl/ndl-topology.owl#> .
@prefix nml: <http://schemas.ogf.org/nml/2013/05/base#> .
@prefix owl: <http://www.w3.org/2002/07/owl#> .
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@prefix sdndl: <http://www.gsi.dit.upm.es/ontologies/sdndl#> .
@prefix sdndlcao: <http://www.ctb.upm.es/ontologies/sdndlcao#> .
@prefix xml: <http://www.w3.org/XML/1998/namespace> .
@prefix xsd: <http://www.w3.org/2001/XMLSchema#> .

sdndlcao:device_14-7d-da-e0-71-34 rdf:type owl:NamedIndividual ,
                                          ndl-topology-owl:Device ,
                                          nml:Node ;
        sdndlcao:deviceOfSnapshot sdndlcao:snapshot_d5e21d4f31f1894be94735d354bce24d7a694a2100e451ee86f6f0d08e031815 ;
        sdndl:ipAddress "192.168.50.20"^^xsd:string ;
        sdndlcao:hostname "192.168.50.20"^^xsd:string ;
        sdndlcao:macManufacturer "None"^^xsd:string ;
        sdndlcao:operatingSystem "None"^^xsd:string ;
        sdndlcao:timestampScanEnd "2021-03-23 11:19:18"^^xsd:dateTimeStamp ;
        sdndlcao:timestampScanStart "2021-03-23 11:17:02"^^xsd:dateTimeStamp ;
        dc:identifier "14-7d-da-e0-71-34"^^xsd:string ;
        sdndl:hardwareAddress "14-7d-da-e0-71-34"^^xsd:string ;
        rdfs:label "device_14-7d-da-e0-71-34"@en .
```

Fig. 2 Example of a named individual of SDNDL-CAO class device. Triples providing information of the particular device are included in Turtle format (https://www.w3.org/TR/turtle/). SDNDL-CAO, Software Defined Networking Description Language—CUREX Asset Discovery Tool Ontology.

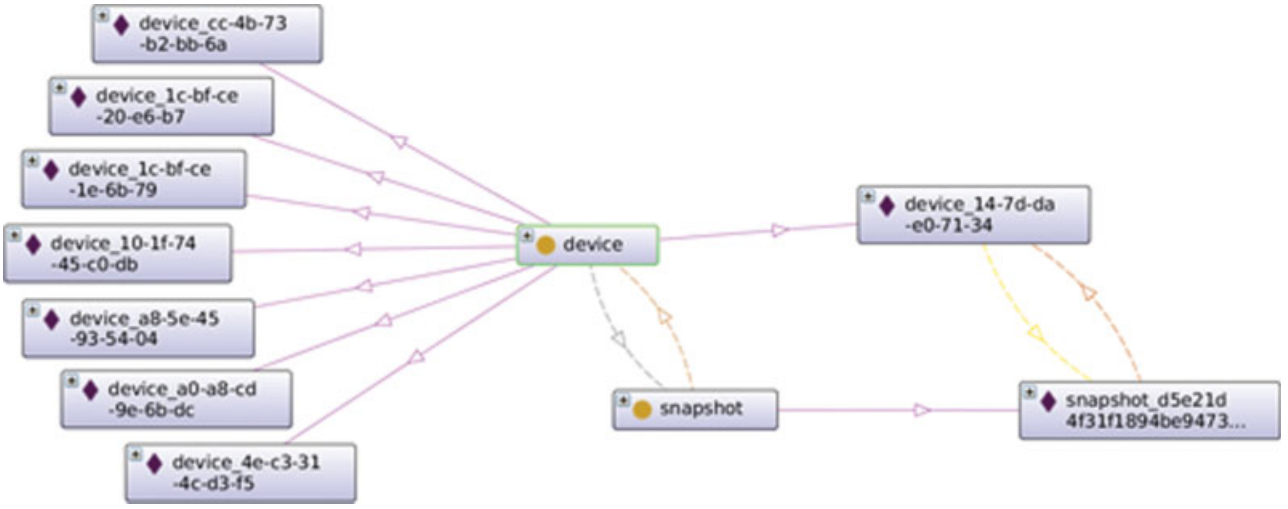

Fig. 3 Example of a partial visualization of SDNDL-CAO classes (in yellow) and instances (in purple). All the named individuals of class device are represented. The snapshot instance(s) of a particular device individual are included. The visualization has been generated with OntoGraf. The representation is a partial simplification of the complete model and instances. SDNDL-CAO, Software Defined Networking Description Language—CUREX Asset Discovery Tool Ontology.

Discussion

In the present paper, a new knowledge representation ontology-based model has been proposed. The ontological schema, named SDNDL-CAO, follows the specifications and standards of semantic designs and linked data needs, reusing previous representations and extending those when necessary. The ontology has been developed to model data regarding computer networks within the context of distributed health care environments' cybersecurity. More particularly, the scope of the work is under the CUREX project and semantic data are stored to gather information about assets, devices, open ports and so on, connected to interfaces to find vulnerabilities in the system that could risk critical health care information infrastructures. This way, we propose a semantic representation model that is

```
PREFIX ndl-topology-owl: <http://cinegrid.uvalight.nl/owl/ndl-topology.owl#>
PREFIX nml: <http://schemas.ogf.org/nml/2013/05/base#>
PREFIX sdndl: <http://www.gsi.dit.upm.es/ontologies/sdndl#>
PREFIX sdndlcao: <https://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#>

SELECT DISTINCT STR(?vlan_id) AS ?vlan_id
                STR(?snapshot_id) AS ?snapshot_id
                STR(?timestamp_dist_node_start) AS ?timestamp_dist_node_start
                STR(?timestamp_dist_node_end) AS ?timestamp_dist_node_end

WHERE
      {
      ?interface_instance a  ndl-topology-owl:Interface;
                          sdndlcao:vlanId ?vlan_id;
                          sdndl:hasSnapshot ?snapshot_instance.
      ?snapshot_instance sdndlcao:snapshotId ?snapshot_id;
                         sdndlcao:snapshotOfScanningDevice ?scanningDevice_instance.
      ?scanningDevice_instance sdndlcao:timestampScanStart ?timestamp_dist_node_start;
                               sdndlcao:timestampScanEnd ?timestamp_dist_node_end
      }
```

vlan_id	snapshot_id	timestamp_dist_node_start	timestamp_dist_node_end
vlan_2	05c18c96f2a9be90ada6823f69399d078a6f5fcc1c14602eb2b92f7138ced5ae	2021-03-23 11:46:50	2021-03-23 12:02:03
vlan_2	d5e21d4f31f1894be94735d354bce24d7a694a2100e451ee86f6f0d08e031815	2021-03-23 11:16:49	2021-03-23 11:19:18

Fig. 4 SPARQL query and data returned about VLANs information.

able to embed data coming from distributed systems in hospitals and other health care institutions related to networks' topologies and assets when searching for security or privacy vulnerabilities.

Three main previously developed ontologies have been reused in the present one: NML, NDL, and SDNDL, as they mostly modeled the needed conceptualizations. However, some classes, object properties, and data properties have been specifically created for SDNDL-CAO, since they were not present in the previous ontologies and were needed to represent knowledge in the current one.

When developing SDNDL-CAO, FAIR guidelines have been followed. This means that all semantic data collected in the triplestore comply with findable, accessible, interoperable, and reusable conditions, improving and enhancing this way the integration and understanding of such information. This led us to one of the main advantages of the present approach: the possibility of integrating semantic data from different sources and locations by means of federated queries. Those queries allow users to combine the information from different institutions, not necessarily, held in the same machine, with their own data thanks to the given common ontology. Moreover, the meaning of the data are given in the ontological layer, allowing the anonymization of the information in the individuals' layer.

In the Results section, we have explained the different parts of SDNDL-CAO, including reused and created classes, object properties, and data properties. Some actual scanning instances of a real network have been exemplified to illustrate the utilities of the semantical point of view in this kind of data. In addition, interesting SPARQL queries have been presented, which could be performed in a federated way if applicable.

It is worth commenting that, in the proposed model, temporality representation has been simplified as data properties ("timestampScanStart" and "timestampScanEnd"), which do not allow representing axioms and thus implementing inferences. Temporal characterization could be improved by representing it with other kind of entities enabling more complex reasoning and inferences. An example of how time might be modeled can be found in Batsakis et al.[27]

To the best of our knowledge, there is not a system that works across health institutions' networks by representing the knowledge gathered from discovering network assets' vulnerabilities in a semantical manner. The scientific community can take advantage of ontological representation models used in the intersection of network management and medical informatics. The scheme would allow accessing it in a manner that could provide large amounts of information, given that it can retrieve data from other databases and

```
PREFIX ndl-topology-owl: <http://cinegrid.uvalight.nl/owl/ndl-topology.owl#>
PREFIX nml: <http://schemas.ogf.org/nml/2013/05/base#>
PREFIX sdndl: <http://www.gsi.dit.upm.es/ontologies/sdndl#>
PREFIX sdndlcao: <https://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>

SELECT DISTINCT STR(?vlan_id) AS ?vlan_id
                STR(?node_ip_address) AS ?node_ip_address
                STR(?timestamp_dist_node_scan_start) AS ?timestamp_dist_node_scan_start
                STR(?timestamp_dist_node_scan_end) AS ?timestamp_dist_node_scan_end
                STR(?timestamp_device_scan_start) AS ?timestamp_device_scan_start
                STR(?timestamp_device_scan_end) AS ?timestamp_device_scan_end
                STR(?mac_address) AS ?mac_address
                STR(?mac_manufacturer) AS ?mac_manufacturer
                STR(?ip_address) AS ?ip_address
                STR(?operating_system) AS ?operating_system
                STR(?hostname) AS ?hostname
                STR(?port) AS ?port
                STR(?service) AS ?service
                STR(?service_version) AS ?service_version
                STR(?discovery_method) AS ?discovery_method
                STR(?state) AS ?state
                STR(?protocol) AS ?protocol

WHERE
      {
      ?snapshot_instance sdndlcao:snapshotId "05c18c96f2a9be90ada6823f69399d078a6f5fcc1c14602eb2b92f7138ced5ae"^^xsd:string;
                         sdndl:isSnapshotOf ?interface_instance;
                         sdndlcao:snapshotOfScanningDevice ?scanningDevice_instance;
                         sdndlcao:snapshotOfDevice ?device_instance;
                         sdndlcao:snapshotOfDiscoveringService ?discoveringService_instance.

      ?interface_instance sdndlcao:vlanId ?vlan_id;
                          sdndl:ipAddress ?node_ip_address.

      ?scanningDevice_instance sdndlcao:timestampScanStart ?timestamp_dist_node_scan_start;
                               sdndlcao:timestampScanEnd ?timestamp_dist_node_scan_end.

      ?device_instance sdndlcao:timestampScanStart ?timestamp_device_scan_start;
                       sdndlcao:timestampScanEnd ?timestamp_device_scan_end;
                       sdndl:hardwareAddress ?mac_address;
                       sdndlcao:macManufacturer ?mac_manufacturer;
                       sdndl:ipAddress ?ip_address;
                       sdndlcao:operatingSystem ?operating_system;
                       sdndlcao:hostname ?hostname.

      ?discoveringService_instance sdndlcao:discoveringServiceOfService ?service_instance;
                                   sdndlcao:serviceVersion ?service_version;
                                   sdndlcao:discoveryMethod ?discovery_method;
                                   sdndlcao:state ?state;
                                   sdndlcao:protocol ?protocol.

      ?service_instance sdndl:portNumber ?port;
                        sdndlcao:serviceName ?service.
      }
```

vlan_id	node_ip_address	timestamp_dist_node_scan_start	timestamp_dist_node_scan_end	timestamp_device_scan_start	timestamp_device_scan_end	mac_address
vlan_2	192.168.50.121	2021-03-23 11:46:50	2021-03-23 12:02:03	2021-03-23 11:47:02	2021-03-23 11:48:01	1c-bf-ce-20-e6-b7
vlan_2	192.168.50.121	2021-03-23 11:46:50	2021-03-23 12:02:03	2021-03-23 11:47:02	2021-03-23 11:47:44	1c-bf-ce-1e-6b-79
vlan_2	192.168.50.121	2021-03-23 11:46:50	2021-03-23 12:02:03	2021-03-23 11:47:02	2021-03-23 11:48:00	a8-5e-45-93-54-04
vlan_2	192.168.50.121	2021-03-23 11:46:50	2021-03-23 12:02:03	2021-03-23 11:47:02	2021-03-23 11:48:01	1c-bf-ce-20-e6-b7

mac_manufacturer	ip_address	operating_system	hostname	port	service	service_version	discovery_method	state	protocol
None	192.168.50.121	Linux 2.6.32	dflobon	49158	microsoft-windows-rpc		probed	open	tcp
Shenzhen Century Xinyang Technology Co., Ltd	192.168.50.225	Linux 2.6.32	192.168.50.225	8289	gsoap	2.7	probed	open	tcp
None	192.168.50.1	Linux 2.6.32 - 3.10	router.asus.com	5357	microsoft-httpapi-httpd	2.0	probed	open	tcp

Fig. 5 SPARQL query and part of the data returned about a given snapshot.

```
PREFIX ndl-topology-owl: http://cinegrid.uvalight.nl/owl/ndl-topology.owl#
PREFIX nml: <http://schemas.ogf.org/nml/2013/05/base#>
PREFIX sdndl: <http://www.gsi.dit.upm.es/ontologies/sdndl#>
PREFIX sdndlcao: <https://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>

SELECT DISTINCT STR(?mac_address) AS ?mac_address
                STR(?mac_manufacturer) AS ?mac_manufacturer
                STR(?ip_address) AS ?ip_address
                STR(?operating_system) AS ?operating_system
                STR(?hostname) AS ?hostname
WHERE
      {
      ?service_instance sdndlcao:serviceName "mysql"^^xsd:string;
                        sdndlcao:serviceOfDevice ?device_instance.

      ?device_instance sdndl:hardwareAddress ?mac_address;
                       sdndlcao:macManufacturer ?mac_manufacturer;
                       sdndl:ipAddress ?ip_address;
                       sdndlcao:operatingSystem ?operating_system;
                       sdndlcao:hostname ?hostname.

      }
```

mac_address	mac_manufacturer	ip_address
a0-a8-cd-9e-6b-dc	Intel Corporate	192.168.50.53
1c-bf-ce-1e-6b-79	Shenzhen Century Xinyang Technology Co., Ltd	192.168.50.225

operating_system	hostname
Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1	192.168.50.53
Linux 2.6.32	192.168.50.225

Fig. 6 SPARQL query and returned data about the devices in which a given service is open.

thus can offer much more powerful queries in those interdisciplinary contexts. This was the main motivation under SDNDL-CAO development.

Conclusion

The developed work allows the publication of assets discovery information in networks data, in the context of health care distributed environments cybersecurity, by semantizating information following the proposed ontology. In it, some concepts of previous ontologies have been reused while others have been specifically created. The main contribution of the present study is the suggested model that enable their users to store semantic data regarding assets, devices, interfaces, ports and services when scanning a health care environment network looking for possible cybersecurity vulnerabilities.

Some of the prospective lines to extend the current work could focus on the integration in the present ontology of existing biomedical ontologies representing more clinical and biological information stored in the different assets, thus aggregating both the security network-related data and for instance the patients' data itself kept in the health institutions' devices. Temporality could be represented in a more elaborated way to enable axioms representation and simplify inferences rather than just like data properties. We aim to cover and improve such time aspect in the future. We would also like to develop a more exhaustive evaluation of the maturity of the FAIRness of the suggested ontology. Moreover, other kinds of validation would very much improve our approach: including how the presented ontology works in a real health care scenario will be a very relevant and urgent task.

```
PREFIX ndl-topology-owl: http://cinegrid.uvalight.nl/owl/ndl-topology.owl#
PREFIX nml: <http://schemas.ogf.org/nml/2013/05/base#>
PREFIX sdndl: <http://www.gsi.dit.upm.es/ontologies/sdndl#>
PREFIX sdndlcao: <https://medal.ctb.upm.es/projects/CUREX/ontologies/sdndlcao#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>

SELECT DISTINCT STR(?mac_address) AS ?mac_address
                STR(?snapshot_id) AS ?snapshot_id
WHERE
{
?device_instance sdndlcao:deviceOfSnapshot ?snapshot_instance;
                 sdndl:hardwareAddress ?mac_address.
?snapshot_instance sdndlcao:snapshotId ?snapshot_id.

        {
        SELECT DISTINCT ?device_instance
                        (COUNT(?device_instance) AS ?num_snapshots)
        WHERE {
                ?device_instance a ndl-topology-owl:Device;
                                 sdndlcao:deviceOfSnapshot ?snapshot_instance.
                }
        GROUP BY ?device_instance
        HAVING COUNT(?device_instance) > 1
        }
}
```

mac_address	snapshot_id
10-1f-74-45-c0-db	d5e21d4f31f1894be94735d354bce24d7a694a2100e451ee86f6f0d08e031815
1c-bf-ce-1e-6b-79	05c18c96f2a9be90ada6823f69399d078a6f5fcc1c14602eb2b92f7138ced5ae
14-7d-da-e0-71-34	d5e21d4f31f1894be94735d354bce24d7a694a2100e451ee86f6f0d08e031815
1c-bf-ce-20-e6-b7	d5e21d4f31f1894be94735d354bce24d7a694a2100e451ee86f6f0d08e031815
10-1f-74-45-c0-db	05c18c96f2a9be90ada6823f69399d078a6f5fcc1c14602eb2b92f7138ced5ae
a8-5e-45-93-54-04	05c18c96f2a9be90ada6823f69399d078a6f5fcc1c14602eb2b92f7138ced5ae
a8-5e-45-93-54-04	d5e21d4f31f1894be94735d354bce24d7a694a2100e451ee86f6f0d08e031815
1c-bf-ce-20-e6-b7	05c18c96f2a9be90ada6823f69399d078a6f5fcc1c14602eb2b92f7138ced5ae
cc-4b-73-b2-bb-6a	d5e21d4f31f1894be94735d354bce24d7a694a2100e451ee86f6f0d08e031815
1c-bf-ce-1e-6b-79	d5e21d4f31f1894be94735d354bce24d7a694a2100e451ee86f6f0d08e031815

Fig. 7 SPARQL query and data returned about devices scanned in multiple snapshots.

Funding

The research work presented in this article has been supported by the European Commission under the Horizon 2020 Programme, through funding of the CUREX project (G.A. n 826404).

Conflict of Interest

None declared.

References

1 Sørensen C, de Reuver M, Basole RC. Mobile Platforms and Ecosystems. J Inf Technol 2015;30(03):195–197

2 Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare challenges in the era of cybersecurity. Health Secur 2020;18(03):228–231

3 Critical Infrastructures and Services. Accessed April 13, 2021 at: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services

4 Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection (Text with EEA Relevance). Vol OJ L.; 2008. Accessed April 13, 2021 at: http://data.europa.eu/eli/dir/2008/114/oj/eng

5 Shi F, Li Q, Zhu T, Ning H. A survey of data semantization in internet of things. Sensors (Basel) 2018;18(01):E313

6 Kaur K, Rani R. Managing data in healthcare information systems: many models, one solution. Computer 2015;48(03):52–59

7 Chen P-T, Lin C-L, Wu W-N. Big data management in healthcare: adoption challenges and implications. Int J Inf Manage 2020; 53:102078

8 Kolias VD, Stoitsis J, Golemati S, Nikita KS. Utilizing semantic web technologies in healthcare. In: Koutsouris D-D, Lazakidou AA, eds. Concepts and Trends in Healthcare Information Systems. Annals of Information Systems Springer International Publishing; 2014:9–19

9 Hammad R, Barhoush M, Abed-Alguni BH. A semantic-based approach for managing healthcare big data: a survey. J Healthc Eng 2020;2020:8865808

10 Kim DJ, Hebeler J, Yoon V, Davis F. Exploring determinants of semantic web technology adoption from IT professionals' perspective: industry competition, organization innovativeness, and data management capability. Comput Human Behav 2018;86:18–33

11 Guarino N. Formal Ontologies and Information Systems. IOS Press; 1998

12 Guarino N, Oberle D, Staab S. What is an ontology? In: Staab S, Studer R, eds. Handbook on Ontologies. International Handbooks on Information Systems. Berlin, Heidelberg: Springer; 2009:1–17

13 RDF - Semantic Web Standards Published November 24, 2019. Accessed November 24, 2019 at: https://www.w3.org/RDF/

14 SPARQL Query Language for RDF Published November 24; 2019. Accessed November 24, 2019 at: https://www.w3.org/TR/rdf-sparql-query/

15 Wilkinson MD, Dumontier M, Aalbersberg IJ, et al. The FAIR Guiding Principles for scientific data management and stewardship. Sci Data 2016;3:160018

16 OpenLink Virtuoso Universal Server Documentation Published November 25, 2019. Accessed November 25, 2019 at: http://docs.openlinksw.com/virtuoso/

17 Antoniou G, van Harmelen F. Web Ontology Language: OWL. In: Staab S, Studer R, eds. Handbook on Ontologies. International Handbooks on Information Systems. Berlin, Heidelberg: Springer; 2004:67–92

18 Zhou Q, Gray AJG, McLaughlin S. ToCo: An ontology for representing hybrid telecommunication networks. In: Hitzler P, Fernández M, Janowicz K et al, eds. The Semantic Web: 16th International Conference, ESWC 2019, Portorož, Slovenia, June 2–6, 2019. Series: Lecture Notes in Computer Science (11503). Springer; 507–522

19 Sikos LF, Stumptner M, Mayer W, Howard C, Voigt S, Philp D. Representing network knowledge using provenance-aware formalisms for cyber-situational awareness. Procedia Comput Sci 2018;126:29–38

20 Mozzaquatro BA, Agostinho C, Goncalves D, Martins J, Jardim-Goncalves R. an ontology-based cybersecurity framework for the internet of things. Sensors (Basel) 2018;18(09):E3053

21 Herzog A, Shahmehri N, Duma C. An ontology of information security. IJISP 2007;1:1–23

22 Voigt S, Howard C, Philp D, Penny C. Representing and reasoning about logical network topologies. In: Croitoru M, Marquis P, Rudolph S, Stapleton G, eds. Graph Structures for Knowledge Representation and Reasoning. Lecture Notes in Computer Science. Springer International Publishing; 2018: 73–83

23 Intelligent Systems Group. Software defined networking description language. Accessed March 5, 2021 at: http://www.gsi.upm.es/ontologies/sdndl/

24 Grosso P, Dijkstra F, Van der Ham J, Laat C. Network description language–semantic web for hybrid networks. Proceedings of TERENA Networking Conference 2007. Kongens Lyngby, Copenhagen, Denmark

25 Ghijsen M, van der Ham J, Grosso P, de Laat C. Towards an infrastructure description language for modeling computing infrastructures. Paper presented at: 2012 IEEE 10th International Symposium on Parallel and Distributed Processing with Applications; 2012:207–214

26 van der Ham J, Dijkstra F, Lapacz R, Brown A. The network markup language (nml) a standardized network topology abstraction for inter-domain and cross-layer network applications. Paper presented at: Proceedings of the 13th TERENA Networking Conference, Maastricht, Netherlands; 2013

27 Batsakis S, Petrakis EGM, Tachmazidis I, Antoniou G. Temporal representation and reasoning in OWL 2. Semant Web 2017;8(06): 981–1000