2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4) | 978-1-6654-0096-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/WorldS451998.2021.9514051

HOPPy: Holistic Ontology for Privacy-Preserving in Smart Healthcare environment

Driss EL MAJDOUBI, Hanan EL BAKKALI, Souad SADKI, Asmae LEGHMID, Zaina MAQOUR
Smart Systems Laboratory- Rabat IT Center
Mohammed V University in Rabat
{Driss.elmajdoubi, h.elbakkali,souad.sadki}@um5s.net.ma,{asmae_leghmid, zaina_maqour }@um5.ac.ma

***Abstract*—Nowadays, the Internet of Things (IoT) have a great impact on improving the quality of patients' lives and offering advanced healthcare services. In this context, Smart Healthcare (S-healthcare) is an important domain with a massive knowledge base, to perform continuous health monitoring, and to provide hopeful solutions that can effectively give perfect and innovative health-related services to patients. However, due to the diversity of stakeholders involved in patients' care and the huge amount of health data collected by Medical IoT devices, the use of s-healthcare applications raises significant issues and risks in terms of privacy. In this paper, we propose a holistic privacy ontology for privacy-preserving in a S-healthcare environment. Our proposed ontology aims at defining a common privacy vocabulary in order to meet the privacy needs of the different stakeholders especially the accordance of privacy policies with patients' preferences and with the main privacy laws and regulations. Experimental results show that the proposed ontology is feasible for S-healthcare environment.**

Keywords—Smart Healthcare, Privacy Level Agreement, Privacy Policy, Privacy Preferences, Ontology, Privacy Laws, IoT

I. INTRODUCTION

Healthcare services are among the most needed and consumed services in the world. Besides improving this significant domain, healthcare systems should be upgraded to permit global health monitoring and synchronous detection of urgent health conditions.

The idea of smart healthcare is examined as a novel thought for implementing a healthcare system based on the internet of things (IoT). IoT connects all categories of data acquisition instruments (IoT devices, sensors, and actuators) effectively and provides a smart and connected HealthCare [16]. In smart healthcare systems, IoT applications allow the exchange of diversified data between different actors across communication protocols. Yet, this communication can lead to privacy violation risks [17].

Researchers are exploiting the power of IoT technologies in the healthcare domain. Accordingly, privacy protection becomes harder to manage because of the huge amount of sensitive information generated, transferred, and stored in different locations and cloud architectures. In fact, privacy preserving is a time-consuming task that requires a lot of effort and knowledge. Particularly in Smart healthcare, this knowledge dimension has not been given particular attention. Hence, in order to effectively manage privacy; the first step consists of understanding and then defining the basic concepts needed to describe privacy requirements. To achieve this, many privacy ontologies have been proposed trying to cover some or all terminology of healthcare, but still needs practical evaluation to improve the preservation of the data owner's privacy in a smart healthcare environment.

In another line, the regulatory pressure and the privacy violation risks urge both the patients and the Smart Healthcare providers to ensure the data privacy preserving [10]. However, ensuring the accordance between the patient's preferences and the S-health provider's privacy policies requires the use of a common privacy vocabulary that describes the privacy requirements. This accordance enables the creation of a common Privacy policy called « Privacy Level Agreement » (PLA) settled between patient and s-healthcare provider that can be applied to preserve the data privacy in the Smart Healthcare environment.

To the best of our knowledge, we proposed the first ontology combing both Smart Healthcare and IoT vocabularies. This combination will facilitate the understanding and the expression of patient's privacy preferences in a smart environment. More interestingly, our suggested solution takes third parties' privacy policies for granted. Therefore, verifying the accordance of these policies to patients' privacy preferences becomes easier on one hand and their compliance to laws and regulations on the other hand [18].

To express such privacy vocabulary, we suggest a Holistic Ontology for Privacy-Preserving in a Smart Healthcare environment, called HOPPy. This ontology intends to pinpoint the main privacy requirements from the different stakeholders' points of view and during the whole Medical IoT data lifecycle, including the collection, transmission, storage, and processing phases.

The rest of this paper is organized as follows. In Section 2 we provide an overview of the literature and related papers. The proposed ontology, called HoPPY for privacy-preserving is then described in Section 3. Section 4 presents the phase of the implementation and evaluation, and section 5 concludes the paper and presents future work.

II. RELATED WORKS

This section illustrates the main ontologies and terminologies that have been proposed to express the research area. This research work integrates three different classes of ontologies, (i) Healthcare and medical IoT-based ontologies, (ii) Privacy-aware based ontologies, and (iii) IoT-privacy-based ontologies.

A. Healthcare and medical IoT based ontologies:

Over the last years, several ontologies and terminologies in the healthcare domain have been proposed. The most important ones are the International Classification of Diseases (ICD) [1], a terminology that introduces the standard diagnostic for all general diseases, and symptoms. Another standard called Systematized Nomenclature of Medicine - Clinical Terms (SNOMED CT) [2] was proposed converging most medical terms while offering a semantic classification.

Nevertheless, these works have various issues; they are based on medical terms and patient medical records without having new technologies such as IoT, SWoT in the healthcare domain. Moreover, they did not handle customer preferences, which is a fundamental right that must be granted to all people.

To offer better healthcare services, we need to design new healthcare systems using the Internet of Things and semantic web for a perfect representation of data. Ben Elhadj et al. [3] highlighted an ontology which is constructed by the integration of other existing ontologies related to healthcare-IoT-based systems. Despite the improvement brought by this research, they just focus on the healthcare and medical-IoT terminologies. Besides, privacy requirements of personal data are ignored. In a continuation of the previous work, Ben Elhadj et al.[4] proposed Do-Care; an ontology reasoning-based healthcare monitoring system. The proposed system is developed to support the supervision of patients suffering from chronic diseases. Still, this solution did not guarantee privacy preferences and protect sensitive data.

Tiwari et al. [5] have presented a healthcare ontology HCI-oTO for transferring the collected data from medical devices to the knowledge base. They have presented a semantic model with security layers interconnected with IoT devices. However, the researchers are harnessing the power of IoT in HealthCare, and they maintain the security in IoT-based health devices. But still, there is a need to ensure compliance with privacy preferences and legal regulations.

B. Privacy-aware based ontologies:

Hosseinzadeh et al. [6] used Smart-M3 platform, to protect privacy of users. Authors modeled an access control scheme-Context Aware Role-Based Access Control (CARBAC) via ontological modeling techniques and proposed an OWL ontology that integrated CLIPS rules. The proposed ontology has various restrictions including the implemented privacy is limited to access control and it is not compliant with the legal regulations or considers the user preferences.

Zhang et Todd. [7] addressed the context-awareness systems and personal privacy protection. They introduced automated processes in privacy control, by developing a privacy ontology, which is based on the terminology and policies specified inW3C's Platform for Privacy Preferences (P3P). This ontology tried to cover privacy policies and user's preferences while neglecting the privacy laws, besides, it meant for context-aware systems and may not apply to a smart healthcare environment.

Sacco et Passant. [8] proposed an ontology called the Privacy Preference Ontology (PPO) that enables users to create fine-grained privacy preferences, that can restrict access to their sensitive data.Though, the proposed ontology only allows privacy preferences and does not consider privacy regulations and laws requirements.

Bhatia et Singh.[9] proposed a framework that solves the client's privacy protection dilemma in the context of the web services paradigm, and implemented it using OWL and semantic web rule language SWRL to formulate the user's preferences. However, the privacy requirements are not proposed by law regulations, and this solution is designed for web services and not for medical IoT or smart healthcare.

C. IoT-privacy based ontologies:

Loukil et al. [10] proposed an ontology-based privacy-preserving named LIoPY, which gives the right to the user to set his preferences and then match them with the access query of the requester by using semantic modeling, and standard ontology languages. However, the defined privacy requirements are based on European legislation, thus several questions arise about this ontology compatibility with other laws. An extension of the previous work was proposed in [11],where they introduced an IoT data privacy-preserving framework, called PrivBlockchain to enforce privacy. Yet, the lack of the features mentioned above is always maintained.

Agarwal et al. [12] The proposed ontology is designed for IoT, and inspired by the GDPR and ISO/IEC 29100 to set the privacy concepts, but it doesn't cover privacy during the full data cycle, they focused only on data gathering and sharing phases, and they didn't mention the right of setting preferences by the users.

To conclude based on all the existing ontologies mentioned above and their comparison presented in table 1, we can observe that there is not a holistic ontology that is addressed for preserving privacy in smart healthcare. The existing ontologies either focused on healthcare and medical IoT or focused on privacy support. Hence, it emerges necessarily to suggest a holistic solution that takes into account the different issues of the aforementioned stakeholders. More interestingly, this solution has to consider the accordance of privacy policies with users' preferences and the compliance with privacy laws and regulations. Therefore, we propose HOPPy, a holistic ontology that covers the whole context of privacy in a smart healthcare environment.

III. Overview of the proposed ontology (HOPPy)

To be compliant with today's ontology engineering, we adopt the METHONTOLOGY methodology, which consists of building an ontology from scratch. In order to cover the whole smart healthcare privacy aspects, HOPPy contains two main modules, namely smart healthcare description module and smart healthcare privacy management module. Figure 1 presents the different HOPPy's modules.

TABLE I. EXISTING HEALTHCARE AND MEDICAL IOT ONTOLOGIES COMPARISON.

	Healthcare Description	IoT Description	Privacy Support		Privacy regulations and laws requirements		
			Privacy Preferences	Privacy Policy	GDPR Compliance	HIPAA Compliance	Law 09-08 Compliance
[1]	+	-	-	-	-	-	-
[2]	+	-	-	-	-	-	-
[3]	+	+	-	-	-	-	-
[4]	+	+	-	-	-	-	-
[5]	+	+	-	-	-	-	-
[6]	-	-	-	+	-	-	-
[7]	-	-	+	+	-	-	-
[8]	-	-	+	-	-	-	-
[9]	-	-	+	+	-	-	-
[11]	-	+	+	+	+	-	-
[12]	-	+	-	+	+	-	-
Ours	+	+	+	+	+	+	+

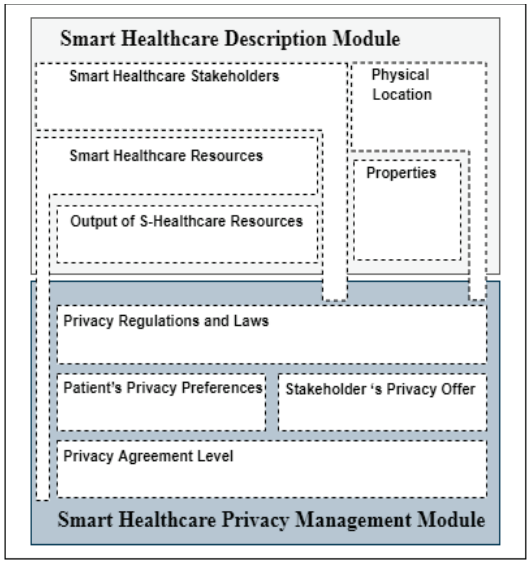

Figure 1: HOPPy's Modules.

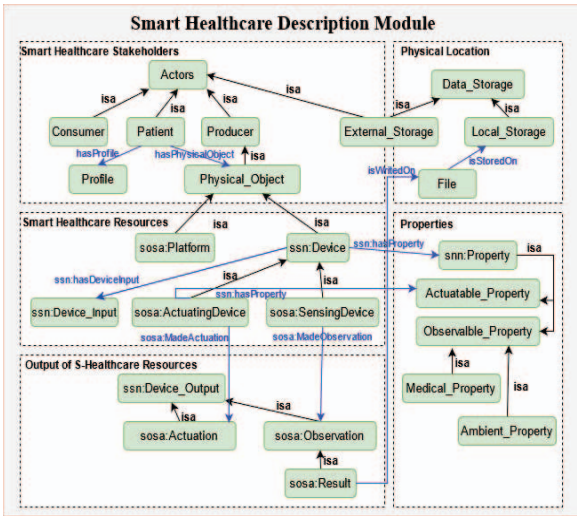

Figure 2: S-Healthcare Description Module in HOPPy.

A. *Smart Healthcare Description Module*

The S-Healthcare description module describes the Smart Healthcare environment. It includes five sub-modules, as illustrated in Figure 1:

1) *Smart Healthcare Stakeholders*

This sub-module integrates the several parties of S-Healthcare data that contains:

(a) Data Producer; several smart devices, it includes:

- SSN:Physical_Object class that represents the objects used to surveil health conditions. It has a Platform subclass that references platforms where different stakeholders exchange feedback and recommendations, and a Device subclass for the different devices used by the data owner in his smart environment.

(b) Data Owner; Patients are the owners of data circulating in the healthcare environment; therefore defining patients' profiles is a required process.

- Patient: class saves information related to the patient; it has several properties:

- HasProfile: relates patients to their profiles.
- HasHealthCondition: links patients to their actual health condition.
- HasService: links patients to the services needed.
- UsePhysicalObject: links patients to their physical Objects.

(c) Data Consumer; medical actors, using data collected by medical devices, can monitor their patients anywhere, anytime and can update prescriptions when needed. ICNP:Individual represents all the possible human actors in a healthcare environment: ICNP:Doctor, ICNP:Nurse, ICNP:Pharmacist, ICNP:CareProvider, etc.

2) Smart Healthcare resources

This sub-module describes different smart healthcare resources, it includes two classes: sosa:SensingDevice and sosa:ActuatingDevice.

- sosa:SensingDevice: used to detect and measure vital signs.
- sosa:ActuatingDevice: used to change the patients' states.

3) Output of S-Healthcare resources

The output of smart healthcare resources describes the results produced, i.e. value of an observation, is represented by the class sosa:Result, and the class sosa:Observation is to estimate or calculate a value of a property of a feature of interest.

4) Properties

Properties, which describes the properties of the smart healthcare resources and their results. This submodule manifests in ssn:Property class that has two sub-classes:

- Observalble_Property class refers to the captured data by the sensing devices. This class has two subclasses (a) Medical_Property that represent medical parameters, and (b) Ambient_Property that describe ambient information.
- Actuatable_Property class defines actuations realized by actuators.

5) Physical location

This submodule involves the storage location of the data owner's preferences, and the output of smart Healthcare resources. It contains the Data_Storage_Location class, which includes External_Storage and Local_Storage sub-classes.

B. Smart Healthcare privacy management module

The S-healthcare privacy management module describes the process of privacy-preserving through Privacy Level Agreement between the patient's preferences and the S-healthcare stakeholders' privacy offer. This module contains four submodules, as illustrated in Figure 3.

1) Privacy regulations and laws

In this sub-module, we tried to set the different regulations and law requirements that should be verified in the privacy policy offered by stakeholders. Therefore we proposed the following classes (i) LIoPY: Privacy_Attribute that was proposed by LIoPY ontology and it covers six principles presented in six sub-classes, Consent, Purpose, Retention, Operation, Condition, and Disclosure, to grant full awareness to the patients of what reason, how long, how, under what circumstances, and to what range their data can be shared. (ii) Privacy_

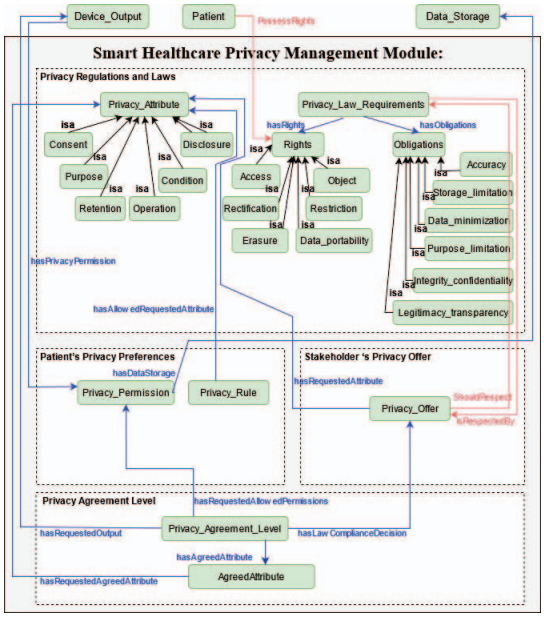

Figure 3: S-Healthcare Privacy Management Module in HOPPy.

Law_Requirements, which contains two, sub-classes namely Rights and Obligations.

(a) Rights Class: Following chapter 3 of the General Data Protection Regulation (GDPR) [13], which describes the rights of the data subject, we proposed six sub-classes to identify the rights of the patients as presented in Table 2.

(b) Obligations Class: According to Art 5 of GDPR, both the data consumer and the data producer have many principles and responsibilities regarding data processing. Table 3 presents these principles, where each one presents a sub-class of Obligations class.

TABLE II. RIGHTS SUB-CLASSES BASED ON [14]

Right of the patient	Description
Access	The data consumers and producers shall provide a copy of the personal data undergoing processing.
Rectification	The right to rectification inaccurate or incomplete data.
Erasure	The patient should have the right to request the erasure of his personal data.
Restriction	The right to restrict the processing of the data in certain conditions declared in Art.18 GDPR.
Data_portability	The right to transfer the data from a stakeholder to another without interfering with others' rights and freedoms.
Object	The right to object the data processing in certain situations declared in Art. 21 GDPR

TABLE III. OBLIGATIONS SUB-CLASSES BASED ON [15]

Obligations	Description
Legitimacy_transparency	The patient can consult at any time his data processing activities.
Purpose_limitation	The usage of the patient's data is limited to the defined purpose.
Data_minimization	The collected information is limited to the required data for processing purposes.
Storage_limitation	The stored data is maintained only during the necessary period to achieve the intended purposes.
Accuracy	The stored data is frequently updated and corrected in case of any inaccuracies.
Integrity_confidentiality	The data is protected from unauthorized access, accidental loss, destruction, or damage.

2) Patient's privacy preferences

In this sub-module, the patients define the set of rules, and preferences regarding their collected data, to restrict its usage by the different stakeholders. it includes two classes, (i) Privacy_Rule where they express the values of the predefined attributes of Privacy_Attribute Class, and it has hasAllowedRequestedAttribute as an object property. (ii) Privacy_Permission where the patient describes he either Permits or Denies the requested permissions, and it possesses the object property hasDataStorage.

3) Stakeholder's privacy offer

This sub-model contains the class Privacy_Offer, which describes the privacy policy offered by the service providers, to define how they will manage the requested data and validates its compatibility with Privacy_Law_Requirements, through the object property ShouldRespect.

4) Privacy Agreement Level

The privacy agreement level sub-module contains one class named Privacy_Agreement, which represents the final generated privacy policy that responds to the patients' hand by matching the privacy attributes mentioned previously. It has four object properties, namely: hasRequestedOutput, hasRequestedAllowedPermissions, hasLawCompliance Decision, and hasAgreedAttribute. The PrivacyAgreement class has a sub-class named Agreed_Attribute with the object property hasRequestedAgreedAttribute.

IV. EXPERIMENTATION

In order to show the relevance and the applicability of our proposed ontology. We present in this section a real-world case study through which we demonstrate how such an ontology as HOPPy can help in modeling the main actors and understanding patient's preferences as well as third parties' privacy policies in a S-health environment. To achieve this, several tools have been used. Firstly, we created our ontology using Protégé [14], an open-source ontology framework used to create, modify, delete, and query concepts and individuals of our HOPPy. Second, in the implementation, we employ the two programming languages OWL and RDF. These languages provide a formal representation enabling the check of inconsistencies, the visualization of the ontology structure, and the ease of maintenance. The implementation phase aims at producing an owl document that defines all HoPPy's terms and inference rules.

A. Smart Healthcare Case Study

James is a 55-year-old man who is overweight, diagnosed with coronary artery disease (CAD), which is a type of heart disease. The first sign of CAD is a heart attack, which means that heart rate should be viewed in the same light as other risk factors. To stay alerted of any symptom, James decided to use a wireless body sensor, to continuously measure his heart rate and his position. These data are sent to the medical center where James is registered so that the doctor can remotely monitor his health.

Therefore, the data stakeholders in this situation are as follows: the **data owner** is James, the **data producer** is the wireless heart rate body sensor, and the **data consumers** are the Health-Monitoring Smart-App, and the medical center. We assume that the **Healthcare Provider** of the "Health Monitoring Smart-App" is called **SH**. Considering the 8 criteria stated in [15], which are compliant with the main privacy law (GDPR), we suggest the following privacy offer.

P1: **HS** says **Smart-App** may disclose data collected from your smart device to other parties for research purposes?

P2: **HS** says **Smart-App** will automatically collect your location and connection.

P3: **HS** says **Smart-App** can use the data for other purposes rather than those related to his healthcare treatment.

P4: **HS** says **Smart-App** will retain your health and no-medical data as long as you use our services.

James's privacy preferences are the following:

P1: **James** says **HS** may disclose my personal data to consumers only.

P2: **James** says **HS** should request my consent before collecting my personal data.

P3: **James** says **HSmay**use the data for treatment purposes only.

P4: **James** says **HS** may retain my health and no-medical data for only 30 days.

After compromising between **James'** privacy preferences and the **HS** service provider's privacy offer, we can come up with the following privacy agreement Level.

P1: **HS** may disclose the collected data to **Smart-App** and **Medical Center**.

P2: **HS** needs the data owner's consent before letting the Smart-App collects the location and the connection data.

P3: **Smart-App** will use the data for healthcare treatment purposes.

P4:**Smart-App** will retain the data owners' health and no-medical for 30 day

Note that the process of compromising between James' privacy preferences and the HS service provider's privacy offer, is carried out usinga set of inference rules and matching algorithm which can be considered as one of our future work.

B. Experimental Results

To validate HoPPy's feasibility, we need to create a HoPPy instance, to translate James's case study, this is possible by using Protégé editor.

In our instance, we can find James as an individual of the Patient class, that has James_Profile, and Heartrate_Sensor, as individuals respectively of Profile class and SensingDevice class. This heart rate sensor has an observation output called James_Heartrate, and an observation result called Result_of_Heartrate_Obsevation, this result is written in James_Personal_File and stored in James_Local_Storage. This information is declared sensitive by James and has a Sensitive_Data_PrivacyRule as an individual of Privacy_Rule class. Besides the privacy rule, James defines a set of permissions in James_Privacy_Permissions as an individual of Privacy_Permission class. On the other hand, the service provider declares his Privacy_Offer_for_Heartrate as an individual of Privacy_Offer class, while respecting the Privacy_Law_Req_for_Heartrate.

After several tests, a Privacy_Agreement_James_Heartrate is generated as compromising privacy between Sensitive_Data_PrivacyRule and Privacy_Offer_for_Heartrate.

To sum up, the obtained results demonstrate the HOPPy feasibility, and capability to be instantiated for privacy-preserving in a smart healthcare environment.

V. Conclusion And future work

In this paper, the proposed ontology is for modeling smart healthcare domains that accord with privacy policies, users' preferences, and compliance with privacy laws and regulations. The ontology is built on various ontologies treating both privacy and the S-healthcare sector.

As a continuation of this work, we are aiming to propose an algorithm that enables matching patient's privacy preferences and service providers' policies using our defined HOPPy ontology. We will also continue to develop a machine-learning algorithm, which serves to predict the patient's privacy preferences based on HOPPy.

References

[1] "International Classification of Diseases, Version 10 - Summary | NCBO BioPortal." https://bioportal.bioontology.org/ontologies/ICD10/ (accessed Feb. 15, 2021).

[2] "SNOMED CT - Summary | NCBO BioPortal." https://bioportal.bioontology.org/ontologies/SNOMEDCT/ (accessed Feb. 15, 2021).

[3] S. TITI, H. B. ELHADJ, and L. CHAARI, "An ontology-based healthcare monitoring system in the Internet of Things," in 2019 15th International Wireless Communications Mobile Computing Conference (IWCMC), Jun. 2019, pp. 319–324, doi: 10.1109/IWCMC.2019.8766510.

[4] H. B. Elhadj, F. Sallabi, A. Henaien, L. Chaari, K. Shuaib, and M. Al Thawadi, "Do-Care: A dynamic ontology reasoning based healthcare monitoring system," Future Generation Computer Systems, vol. 118, pp. 417–431, May 2021, doi: 10.1016/j.future.2021.01.001.

[5] S. Mishra Tiwari, S. Jain, A. Abraham, and S. Shandilya, "Secure Semantic Smart HealthCare (S3HC)," Journal of Web Engineering, vol. 17, pp. 617–646, Jan. 2019, doi: 10.13052/jwe1540-9589.1782.

[6] S. Hosseinzadeh, S. Virtanen, N. Diaz Rodriguez, and J. Lilius, A semantic security framework and context-aware role-based access control ontology for smart spaces. 2016, p. 6.

[7] N. Zhang and C. Todd, "Developing a privacy ontology for privacy control in context-aware systems," p. 4.

[8] O. Sacco and A. Passant, "A Privacy Preference Ontology (PPO) for Linked Data," p. 5.

[9] R. Bhatia and M. Singh, "Privacy Issues in Web Services: An Ontology Based Solution," Procedia Computer Science, vol. 92, pp. 461–467, Jan. 2016, doi: 10.1016/j.procs.2016.07.368.

[10] F. Loukil, C. Ghedira-Guegan, K. Boukadi, and A. N. Benharkat, "LIoPY: A Legal Compliant Ontology to Preserve Privacy for the Internet of Things," in 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Jul. 2018, vol. 02, pp. 701–706, doi: 10.1109/COMPSAC.2018.10322.

[11] F. Loukil, "Towards a new data privacy-based approach for IoT," 2019.

[12] R. Agarwal, T. Elsaleh, and E. Tragos, "GDPR-inspired IoT Ontology enabling Semantic Interoperability, Federation of Deployments and Privacy-Preserving Applications," arXiv:2012.10314 [cs], Dec. 2020, Accessed: Feb. 23, 2021. [Online]. Available: http://arxiv.org/abs/2012.10314.

[13] "Chapter 3 – Rights of the data subject | General Data Protection Regulation (GDPR)." https://gdpr-info.eu/chapter-3/ (accessed Apr. 04, 2021).

[14] M. A. Musen, "The Protégé Project: A Look Back and a Look Forward," AI Matters, vol. 1, no. 4, pp. 4–12, Jun. 2015, doi: 10.1145/2757001.2757003.

[15] A. Subahi and G. Theodorakopoulos, "Ensuring Compliance of IoT Devices with Their Privacy Policy Agreement," in 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Aug. 2018, pp. 100–107, doi: 10.1109/FiCloud.2018.00022.

[16] M.A. Maras, " Internet of things: security and privacy implications, " in International Data Privacy Law 5(2), 99, 2015.

[17] D. E. Majdoubi, H. E. Bakkali and S. Sadki, "Towards Smart Blockchain-Based System for Privacy and Security in a Smart City environment," in 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech), Marrakesh, Morocco, 2020, pp. 1-7, doi: 10.1109/CloudTech49835.2020.9365905.

[18] D. E. Majdoubi and H. E. Bakkali,"Survey of major data privacy laws, languages and approaches in smart cities environments," in 2019, 4th International Conference on Smart city applications (SCA'19), Casablanca, Morocco, 2019, pp. 1-8, doi: 10.1145/3368756.3369013.