Automating Normative Control for Healthcare Research*

Milen G. Kebede[1][0000−0003−4790−7024]

University of Amsterdam, Science Park 904, Amsterdam, Netherlands
m.g.kebede@uva.com

Abstract. There is an increasing need for norms to be embedded in technology as the widespread deployment of big data analysis applications increases. However, existing methodologies do not provide automated policy enforcement mechanisms especially for policies derived from legislation and contractual agreements. Consequently, data access is hindered and collaborations derailed due to fear data misuse and high non-compliance fees. This research aims to automate normative controls in healthcare, such as data sharing agreements, and ultimately, enforce these policies for compliant data usage and access which encourages collaboration and facilitates research outcomes while maintaining accountability. This paper outlines the PhD research questions, current approaches and preliminary results.

Keywords: Policy specification language · Ontology · Access Control Model.

1 Problem statement

In several domains of application, easier accessibility to data has the potential to produce a decisive positive impact [35] . This is particularly true in healthcare research. Current IT infrastructures used by organisations in the healthcare domain to run their business processes typically rely on specific access-control methods, such as the Role based access control model(RBAC), that employ static policies[30]. However, the introduction of legislation such as the General Data Protection Regulation (GDPR)[1] in to this systems creates more complexities due to the complexity and dynamic nature of such normative artefacts. This creates the need for patient data registry maintainers to develop data sharing infrastructures that enforces privacy policies derived from legislation and data sharing agreements, to ensure compliance and encourage collaborative research.

While data sharing encourages collaboration, improves treatment outcomes and maintain accountability, it can also create the opportunity for misuse of data. Data sharing agreements are signed with the goal of preventing misuse

* This work is part of the Enabling Personalized Interventions (EPI) project andis supported by NWO in the Commit2Data –Data2Person program under contract 628.011.028.

and complying with regulations. These agreements regulate contracting parties on how they can share data with each other[21]. Enforcing this agreements is a challenging task considering the complexity of the legal documents. This results in a more cautious and conservative behaviours among data registry maintainers which forces data to stay in silos. Similarly, collaboration between different stakeholders is discouraged due to the challenges of maintaining trust in an environment where decisions can not be traced at system level. Being able to trace back the source of a problem is a necessary requirement for responsibility attribution; lack of this function is detrimental to social maintenance.

On the other hand, current IT infrastructures are not able to take into account that access and use of data is regulated at several levels, whose normative sources (users' consent, contractual agreements, laws) will change in time. Therefore, there is a need for new techniques to automatically enforce policies extracted from these agreements as well as abstract over the complexity of the documents and capture dynamic aspects of policies. This research addresses the challenges of automating privacy policies from legislation and contractual agreements and the automatic enforcement of these policies using an access control mechanism. Identifying the rules relevant to an access request can be challenging, given there are several normative dispositions that may be applicable. Additionally, when rules are taken from different sources, inconsistent policies result in conflict. In the following section, current work in legal ontologies, policy specification langauges and access control models will be presented.

2 Related work

2.1 Legal Ontologies

To address the research goal, existing work on legal ontologies, policy specification languages and access control models is addressed.

Several ontologies are developed to model data-sharing agreements, some of which are designed to regulate data usage and privacy-aware data access[19], to specify contracts, to manage data-flows designed for linked open data environments [12] and to provide legal knowledge modelling of the GDPR core concepts [25]. In general, ontologies have gained momentum in recent years due to their potential as tools to conceptualize and specify shared knowledge as well as organize information, and to reduce the complexity of knowledge management and engineering. These ontologies are tailored to model general or specific kinds of legal knowledge. The LKIF core ontology is a library of ontologies relevant for the legal domain[13]. It can serve as a resources for legal inference, it facilitates knowledge acquisition, and can serve as a basis for semantic annotation of legal information sources.

The LegalRuleML aims to model the interpretation of a rule, the temporal evolution of norms and provides a classification of deontic operators[4]. It encourages the effective exchange and sharing of legal knowledge and reasoning between legal documents, business rules, and software applications. The work on

[25] introduces Pronto which is a legal ontology which provides legal knowledge modelling of the core concepts of General Data Protection Regulation (GDPR). It models deontic concepts and uses the LKIF core ontology to model actions and roles. The UFO-L core ontology represents rights and duty relations and aimes at making more explicit the elements of legal relations [11]. Ontologies are also used to support the application of data-sharing agreements(DSA) in a collaborative health research data sharing scenario by providing the appropriate vocabulary and structure to log privacy events in a linked data based audit log [19].

2.2 Policy specification

A right expression language (REL) is a machine-readable language used typically in digital rights management systems for regulating usage and access control of digital assets. There are several applications to rights expression languages such as stating copyright and expression of contractual language. Some example of RELs are the Extensible Access Control Markup Language (XACML), Enterprise Privacy Authorisation Language (EPAL), and the Open Digital Rights Language (ODRL)[2] [3] [26]. The goal in this research is to utilize a language that supports specifying normative constructs as those specified in privacy regulations and agreements. While extended versions of XACML support partial specification and enforcement of laws and regulations, it lacks for the support for "system obligations" [18]. These are obligations the system has to perform on certain events such as notification of data breach. On the other hand, EPAL is designed for writing enterprise privacy policies but lacks reasoning support for conflicts or other relevant constructs.

RELs are also used for governance in multimedia assets and intellectual property protected content. The work on [28] present the MPEG-21 contract ontology (MCO), a part of the standard ISO/IEC 21000. MCO is an ontology that represents contracts that describe rights on multimedia assets and intellectual property protected content. It describes the contract model and key elements such as the parties in the contract and the relevant clauses conveying permissions, obligations and, prohibitions. Another work [29], presents a dataset of licenses for software and data, expressed as RDF for use with resources on the web. They use ODRL 2.0 to describe rights and conditions present in licenses. It provides a double representation for humans and machines alike and can enable generalized machine-to-machine commerce if generally adopted.

2.3 Access control models

Access control is the process of determining the permissiblity of any access request to perform a specific action on the system such as a read or a write on a data object that belongs to a data subject [5]. Typically, an access control model aims to protect the data object from unauthorized access based on specific access control policies. A number of access control models are proposed to control users' access to data and information resources. The early models presented in

literature include the discretionary access control (DAC) [31], mandatory access control(MAC) [24],and role-based access control (RBAC) [32]. In RBAC, access to various resources is regulated on the basis of the role played by the data-consumer. These models fail to capture the dynamic nature of policies[35]. As a result, the need for flexible and dynamic access control systems has led to the emergence of the attribute-based access control (ABAC) and the usage control model(UCON)[15][38].

Attribute-based access control (ABAC) , is regulated more generally on the basis of the value of attributes of the user while a usage control model (UCON) provides a means for fine grained control over access permissions though attributes. Even though ABAC allows for relationship among parties to be captured, the work in [7] states that ABAC might be lacking when the complexity and dynamically of systems grows thereby making it difficult to capture chains of interpersonal relationships. Other models such as the Relationship-Based Access control, are aimed towards community-centered systems [10]. Access decisions in this model are made based on the social relationships of the parties. This types of models allow for contextual information to be taken into account during access decision making. The gap identified here is the consideration of policies, within access control systems, from various sources of norms which raises the need for policy combination mechanisms as well as conflict resolution mechanism.

3 Research Questions

Given the problem statement and the relevance of this research, the main question this research aims to answer is **how can we develop solutions for the acquisition and application of contractual and other legal requirements for data processing in the healthcare domain, to enable embedded compliance in a distributed data sharing environment?**

Given that our research is restricted to a specific domain, healthcare, the normative artifacts that regulate processing of personal data in this domain need to be identified. After identifying the artefacts, relevant articles and clause that are associated with personal data processing will be extracted. Consequently, the first research question is:

RQ1. Which of the normative artefacts and articles that regulate data sharing systems in the healthcare domain are relevant to this research?

Data sharing systems need to comply with the regulations and data sharing agreements that regulate the parties involved. The policy specification languages utilised to specify such rules need to capture the dynamic nature and complexity of these documents. The policy specification language also should enable a complaint access control mechanism by allowing for the specification of expressive,fine grained and flexible policies. To develop a clear understanding of existing work and identify the relevant policy specification languages, the following research question is derived.

RQ2. What type of policy specification language can be developed or selected from existing languages to specify policies from applicable legislation and contractual agreements in healthcare?

Access control models should manage the complexity and dynamic nature of policies as well as enforcing these policies to ensure compliance. Data sharing systems involve different parties with whom agreements are made. In addition to privacy policies derived from legislation, each party will have their own authorisation requirements to the resources they own which will be specified in the policies. These policies will be composed into a single policy to determine how the asset is utilised. As a result, there is a need to combine these policies and to deal with any inconsistencies that may arise. To mitigate these issues, the third research question is formulated

RQ3 How are policies from various sources of norms combined and inconsistencies handled during access decision making?

4 Proposed Approach

The goal of this research is to capture and enforce normative controls that regulate data sharing infrastructures within healthcare. This research is part of the Enabling Personalised Interventions project(EPI).

The EPI project aims to enable personalised diagnosis by developing real-time monitoring services and digital health twins. EPI aims to empower data subjects and providers through self-management, shared management and personalization across the full health spectrum. It will provide a platform based on secure and trustworthy distributed data infrastructure , that provides actionable and personalised insights for prevention, management and intervention to providers and patients. One of the use cases under EPI is the DIGP registry. Diffuse intrinsic pontine glioma (DIPG) is a rare pediatric brain cancer for which there is no curative treatment, despite decades of clinical trials [37]. In order to advance the progress and pace of DIPG research, the SIOPE DIPG Network and Registry was established. This cancer registry aims to overcome the current lack of clinical, imaging and biologic data and improve academic research on DIPG.

4.1 Identifying regulatory and organizational requirements

The SIOPE DIPG Registry collects information on DIPG patients across Europe and a partner registry in North America, known as the International DIPG Registry, includes patient data from the USA, Canada, Australia and New Zealand. The DIPG network has provided us with different legal documents such as data sharing regulations, data sharing agreements and patient consent forms. Data sharing agreements is an agreement that regulates contracting parties on how they can share data with each other. Its purpose is to define what parties are required to do with respect to condition specified in the agreement [19].

The first stage of this research is to investigate and identify the relevant articles and clauses associated with processing of personal data. Data sharing

agreements consist of terms about the data sharing agreement itself as well as terms concerning the data sharing process. From these documents, relevant articles that specify permissions, prohibitions and obligation will be extracted. Legal documents make references to other legal documents, for example, the data sharing regulation makes several references to the GDPR. Therefore, relevant articles from the GDPR will be extracted. One of the challenges faced during this stage is the difficulty of representing norms accurately due to the complexity of regulatory documents such as the data sharing agreements.

4.2 Formalizing policies from regulatory documents

The readability and usability of the policy specification language plays a central role for interoperability of policies. The goal in this stage is to develop a generic ontology that captures the concept and principles of the GPDR that apply to all context of personal data processing. Additionally, a specialised ontology that captures the concepts and principles of the data sharing agreements will be developed. This may impact the GDPR depending on the interpretation and application of different national and corporate policies. Several policy specification languages will be investigated to identify the ones that fit the use-case requirements. Policy specification languages such as the ODRL, eFlint and XACML are examples of policies investigated through examples from the DIPG use-case.

The policy specification language should also specify both higher and lower level policies . Higher level policies express general level requirements and rights that are specified in legislation , contractual agreements and regulatory requirements. Lower level policies describe how privacy requirements can be implemented in data sharing application such as access control policies. Such policies express what a subject is permitted or prohibited to do in relation to a particular asset e.g a policy that states who can access a certain dataset[22].

4.3 Developing an access control mechanism

The policies from the above ontology will be enforced through an access control mechanism in the data sharing infrastructure. Enforcing policies derived from various norms is not a trivial task. In collaborative data sharing environment, other than the data sharing agreements, parties can also create policies to protect their assets which results in various policies implicating one asset. Some of the existing solutions evaluate the policies of an asset individually,then apply strategies to combine decisions. While others, use an authoritative approach in which policies are combined in a predefined manner[8][20]. These type of approaches will be investigated to determine the policy composition algorithm to be developed.

When policies are derived from various norms, it is possible that we might end up a policy set granting and denying access for the same request to the same asset which creates conflicts. Existing conflict resolution strategies will be investigated. Recent work in this aspect have analysed conflict resolution from a

game theoretic point of view and some graph-theoretic models [14][34][36]. We will investigate existing work and develop conflict resolution strategies.

5 Preliminary results

This section presents our experiences with two policy specification languages in formalizing data sharing scenarios and policies.

5.1 Open Digital Rights Language

In recent years ODRL has gained popularity both in theoretical and practical settings. Our use cases focus on automating data-sharing agreements in the context of healthcare, we found ODRL to be of interest and relevant to our research.

The Open Digital Rights Language (ODRL) is designed as a policy expression language, aiming to provide a flexible and interoperable information model, vocabulary, and encoding mechanism for representing normative statements concerning digital content and services [16]. It evolved through the years from a digital rights expression language for expressing simple licensing mechanisms for the use of digital assets to accommodating privacy policies [17]. The W3C currently supports the ODRL Information Model 2.2 Recommendation. The model is developed using Linked Data principles; however, its semantics is described informally as no formal specification is provided.

Previous work investigated the language's suitability for different scenarios and from different perspectives, and some have proposed the extension of the language [9][33][23]. Our work shares similar motivations, although our analysis focuses on the general modeling process and requirements, as practitioners aiming to model a policy in ODRL. Additionally, vital institutional patterns that were only partially covered before, as delegation, were considered. Delegation is a particularly relevant (and delicate) institutional construct as it brings to the foreground the requirements of meeting the needs of stakeholders while maintaining accountability.

Using ODRL, patterns relevant to data-sharing agreements, highlighting the issues that emerge in the exercises were modelled. The examples were modelled with respect to the ODRL documentations on the information model, informal semantics, use-case and vocabulary of the language. We report our experiences concerning the limitations identified on the current version of the ODRL language. The main limitation identified are: the lack of monotonicity in representing delegation scenarios, semantic ambiguity in the usage of "duty," granularity in identifying parties, and transformational aspects of rules.

5.2 Data sharing policy specification using the eFlint language

Our work describes how data sharing agreements specified using the eFlint language can be used as a means to disseminate certain types of usage and access

control policies. In order to specify data sharing policies, we adopt a domain specific language, eFlint, developed to formalising different sources of norms [6]. The peculiarities of eFlint is that it is an action-based language and that the normative positions of actors are derived from the actions they can perform or are expected to perform. Compliance checking of scenarios and software implementations is simplified because scenarios and software implementation are action based.

It's theoretical foundations are found in transition systems and in Hohfeld's framework for legal fundamental conceptions. This means that eFlint is able to express normative positions,such as, the representation of 'duties' or 'power'. eFlint follows a legal case analysis method that involves interpretation, qualification and assessment of policies. It makes distinction between physical and institutional reality. This realities hold when actors interact with objects , each other and abstractions over physical reality. Additionally, eFlint allows for normative relations to change over time.

In this work, we formalize the semantic of terms, data usage policies and business rules from the data sharing regulation document. The early finding from this work demonstrates that eFlint specifications can be re-usable because types in eFlint can be redefined by subsequent type declaration. A generic interpretation can be used by several application by letting each application specialise certain types to the domain of the application. The concepts of the GDPR can be reused across projects by utilising the references the DIPG regulatory document makes to the GDPR. Second, eFlint is flexible, i.e, the language can be used to specify different sources of norm such as the the GDPR, data sharing regulatory documents and access control rules. Additionally, eFlint allows us to make a connection from higher level policies (GDPR) to lower-level policies(access control policies). We found eFlint to be expressive enough to specify granular policies, therefore our current formalisation match the granularity of the document.

6 Conclusion

There is an urgent need to share data among institutions that reside in the same continent as well as institutions across boarders. The motivation for this research is to contribute to one of the FAIR principles of "Accessibility" [1]. Data should be easily accessible especially in the healthcare. While there are several policy specification languages able to express and govern legally binding behaviour within technological environments, there are still some limitations such as the expressivity of the language in terms of capturing legal concepts [27]. One of the goals behind this research is to model a policy language that is able to represent legal fundamental concepts that can be expressive, granular and flexible enough to be used in a distributed environment.

Access control policies should enhance interoperability while being suitable for the underlying domain of application, in this case, healthcare. As such designing the right specification and enforcement mechanism for access control policies will have organizational benefits. Stakeholders should be enabled to de-

fine the structure of their policies in terms of applicable regulation and data sharing agreements to incorporate security, privacy and business requirements into policies. In future work, an evaluation method for the data sharing ontology as well as the access control mechanism will to measure performance overheads and efficiency of deploying access control mechanisms in the EPI distributed data sharing infrastructure.

7 Acknowledgment

This dissertation project is supervised by Prof. Tom van Engers, Dr. L. Thomas van Binsbegen and Dr. Dannis van Vuurden. This research is part of the EPI project and is supported by NWO in the Commit2Data –Data2Person program under contract 628.011.028.

References

1. 2018 reform of eu data protection rules, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes$_e n.pdf$
2. Anderson, A., Nadalin, A., Parducci, B., Engovatov, D., Lockhart, H., Kudo, M., Humenn, P., Godik, S., Anderson, S., Crocker, S., et al.: extensible access control markup language (xacml) version 1.0. OASIS (2003)
3. Ashley, P., Hada, S., Karjoth, G., Powers, C., Schunter, M.: Enterprise privacy authorization language (epal). IBM Research **30**, 31 (2003)
4. Athan, T., Boley, H., Governatori, G., Palmirani, M., Paschke, A., Wyner, A.: Oasis legalruleml. In: Proceedings of the Fourteenth International Conference on Artificial Intelligence and Law. pp. 3–12 (2013)
5. Bertino, E., Bettini, C., Ferrari, E., Samarati, P.: An access control model supporting periodicity constraints and temporal reasoning. ACM Transactions on Database Systems (TODS) **23**(3), 231–285 (1998)
6. van Binsbergen, L.T., Liu, L.C., van Doesburg, R., van Engers, T.: eflint: a domain-specific language for executable norm specifications. In: Proceedings of the 19th ACM SIGPLAN International Conference on Generative Programming: Concepts and Experiences. pp. 124–136 (2020)
7. Crampton, J., Sellwood, J.: Path conditions and principal matching: a new approach to access control. In: Proceedings of the 19th ACM symposium on Access control models and technologies. pp. 187–198 (2014)
8. Damen, S., den Hartog, J., Zannone, N.: Collac: Collaborative access control. In: 2014 International Conference on Collaboration Technologies and Systems (CTS). pp. 142–149. IEEE (2014)
9. De Vos, Kirrane et al., S., Padget, J., Satoh, K.: Odrl policy modelling and compliance checking. In: International Joint Conference on Rules and Reasoning. pp. 36–51. Springer (2019)
10. Gates, C.: Access control requirements for web 2.0 security and privacy. IEEE Web **2**(0), 12–15 (2007)
11. Griffo, C., Almeida, J.P.A., Guizzardi, G.: A pattern for the representation of legal relations in a legal core ontology. In: JURIX. pp. 191–194 (2016)

12. Hadziselimovic, E., Fatema, K., Pandit, H.J., Lewis, D.: Linked data contracts to support data protection and data ethics in the sharing of scientific data. In: SemSci@ ISWC. pp. 55–62 (2017)
13. Hoekstra, R., Breuker, J., Di Bello, M., Boer, A., et al.: The lkif core ontology of basic legal concepts. LOAIT **321**, 43–63 (2007)
14. Hu, H., Ahn, G.J., Zhao, Z., Yang, D.: Game theoretic analysis of multiparty access control in online social networks. In: Proceedings of the 19th ACM symposium on Access control models and technologies. pp. 93–102 (2014)
15. Hu, V.C., Kuhn, D.R., Ferraiolo, D.F., Voas, J.: Attribute-based access control. Computer **48**(2), 85–88 (2015)
16. Iannella, R., Villata, S.: Odrl information model 2.2. W3C Recommendation (2018)
17. Karafili, E., Lupu, E.C.: Enabling data sharing in contextual environments: Policy representation and analysis. In: Proceedings of the 22Nd ACM on Symposium on Access Control Models and Technologies. pp. 231–238 (2017)
18. Leicht, J., Heisel, M.: A survey on privacy policy languages: Expressiveness concerning data protection regulations. In: 2019 12th CMI Conference on Cybersecurity and Privacy (CMI). pp. 1–6. IEEE (2019)
19. Li, M.: Dsap: Data sharing agreement privacy ontology. Ph.D. thesis (2018)
20. Mahmudlu, R., den Hartog, J., Zannone, N.: Data governance and transparency for collaborative systems. In: IFIP Annual Conference on Data and Applications Security and Privacy. pp. 199–216. Springer (2016)
21. Matteucci, I., Petrocchi, M., Sbodio, M.L., Wiegand, L.: A design phase for data sharing agreements. In: Data Privacy Management and Autonomous Spontaneus Security, pp. 25–41. Springer (2011)
22. Mont, M.C., Pearson, S., Creese, S., Goldsmith, M., Papanikolaou, N.: A conceptual model for privacy policies with consent and revocation requirements. In: IFIP PrimeLife International Summer School on Privacy and Identity Management for Life. pp. 258–270. Springer (2010)
23. Nicoletta Fornara, M.C.: Operational Semantics of an Extension of ODRL Able to express Obligation, vol. 1. Springer International Publishing (2018). https://doi.org/10.1007/978-3-030-01713-2, http://dx.doi.org/10.1007/978-3-030-01713-2_13
24. Osborn, S.: Mandatory access control and role-based access control revisited. In: Proceedings of the second ACM workshop on Role-based access control. pp. 31–40 (1997)
25. Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., Robaldo, L.: Pronto: Privacy ontology for legal compliance. Proceedings of the European Conference on e-Government, ECEG **2018-Octob**(April), 142–151 (2018)
26. Pellegrini, T., Schönhofer, A., Kirrane, S., Steyskal, S., Fensel, A., Panasiuk, O., Mireles-Chavez, V., Thurner, T., Dörfler, M., Polleres, A.: A genealogy and classification of rights expression languages - Preliminary results. Jusletter IT (February), 1–8 (2018)
27. Pellegrini, T., Schönhofer, A., Kirrane, S., Steyskal, S., Fensel, A., Panasiuk, O., Mireles-Chavez, V., Thurner, T., Dörfler, M., Polleres, A.: A genealogy and classification of rights expression languages–preliminary results. In: Data Protection/LegalTech-Proceedings of the 21st International Legal Informatics Symposium IRIS. pp. 243–250 (2018)
28. Rodríguez-Doncel, V., Delgado, J., Llorente, S., Rodríguez, E., Boch, L.: Overview of the mpeg-21 media contract ontology. Semantic Web **7**(3), 311–332 (2016)
29. Rodriguez-Doncel, V., Villata, S., Gómez-Pérez, A.: A dataset of rdf licenses. In: JURIX. pp. 187–188 (2014)

30. Rostad, L., Edsberg, O.: A study of access control requirements for healthcare systems based on audit trails from access logs. In: 2006 22nd Annual Computer Security Applications Conference (ACSAC'06). pp. 175–186. IEEE (2006)
31. Sandhu, R., Munawer, Q.: How to do discretionary access control using roles. In: Proceedings of the third ACM workshop on Role-based access control. pp. 47–54 (1998)
32. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-based access control models. Computer **29**(2), 38–47 (1996)
33. Shakeri, S., Maccatrozzo, V., Veen, L., Bakhshi, R., Gommans, L., De Laat, C., Grosso, P.: Modeling and matching digital data marketplace policies. Proceedings - IEEE 15th International Conference on eScience, eScience 2019 pp. 570–577 (2019)
34. Squicciarini, A.C., Shehab, M., Wede, J.: Privacy policies for shared content in social network sites. The VLDB Journal **19**(6), 777–796 (2010)
35. Wilkinson, M.D., Dumontier, M., Aalbersberg, I.J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.W., da Silva Santos, L.B., Bourne, P.E., et al.: The fair guiding principles for scientific data management and stewardship. Scientific data **3**(1), 1–9 (2016)
36. Xiao, Q., Tan, K.L.: Peer-aware collaborative access control in social networks. In: 8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom). pp. 30–39. IEEE (2012)
37. van Zanten, S.E.V., Baugh, J., Chaney, B., De Jongh, D., Aliaga, E.S., Barkhof, F., Noltes, J., De Wolf, R., Van Dijk, J., Cannarozzo, A., et al.: Development of the siope dipg network, registry and imaging repository: a collaborative effort to optimize research into a rare and lethal disease. Journal of neuro-oncology **132**(2), 255–266 (2017)
38. Zhang, X., Parisi-Presicce, F., Sandhu, R., Park, J.: Formal model and policy specification of usage control. ACM Transactions on Information and System Security (TISSEC) **8**(4), 351–387 (2005)