2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS) | 978-1-6654-4399-9/20/$31.00 ©2021 IEEE | DOI: 10.1109/NTMS49979.2021.9432661

A GDPR-Compliant Framework for IoT-Based Personal Health Records Using Blockchain

Bandar Alamri
CSIS and Lero
University of Limerick
Limerick, Ireland
Bandar.Alamri@lero.ie
0000-0002-0334-0372

Ibrahim Tariq Javed
CSIS and Lero
University of Limerick
Limerick, Ireland
Ibrahimtariq.Javed@lero.ie
0000-0002-7030-5200

Tiziana Margaria
CSIS, HRI and Lero
University of Limerick
Limerick, Ireland
Tiziana.Margaria@lero.ie
0000-0002-5547-9739

***Abstract*—An up-to-date personal health record (PHR) system is crucial for people's health. Achieving a reliable PHR system in the e-Health and m-Health era is still a challenge concerning data integration from different EHRs, data interoperability, and enforcing that access to data is fully under the patient's control. We address these challenges by proposing an electronic health wallet (EHW) system that uses emergent decentralized technologies like blockchain and IPFS and adopts health data interoperability standards and technologies like FHIR's APIs. The EHW stands on a GDPR-compliant framework for IoT-based PHR systems that ensures both data privacy and interoperability. The proposed conceptual framework and system architecture provide a comprehensive solution for a patient-centered IoT-based PHR system that preserves data privacy and satisfies the data interoperability needs. By encouraging patients to share their data in a controlled way, also enables health big data analytics by utilizing the IoT data in a privacy-preserving fashion.**

***Index Terms*—EHR, PHR, IoT, data privacy, GDPR, data interoperability, blockchain, access control, big health data, MDD, eXtreme MDD, low-code application development environments, DIME.**

I. Introduction

Many jurisdictions introduced data protection laws to protect and safeguard personal data and their use. In the USA, the Health Insurance Portability and Accountability Act (HIPAA) [1] organizes the process of storing and accessing patient data. In the European Union, the General Data Protection Regulation 2016/679 (GDPR) [2] covers not only patient data but all service users' data. It explicitly defines the individuals' rights in terms of storing, accessing, and sharing data. Service providers must comply with these regulations that aim to eliminate data breaches and illegal uses, at the risk of significant financial fines.

Accessing real-time data is a right governed in the EU by the General Data Protection Regulation (GDPR). According to [3], GDPR concerns not only accessing, storing, and sharing data but also enforcing data portability. This should lead to data interoperability in Personal Health Record (PHR) systems: with portability, the data owner can receive their data in a real-time manner and can share it consensually with other service providers. According to [4], a PHR is defined as "*An electronic application through which individuals can access, manage and share their health information, and that of others for whom they are authorized, in a private, secure, and confidential environment*". Thus, keeping real-time accurate personal health records is crucial for people's health.

PHR systems differ from Electronic Health Record (EHR) systems in three main respects: 1) PHRs, by definition, should be under patients' control, and this makes them compliant with EU's GDPR; 2) PHRs should involve real-time data produced from patients' medical monitoring sensors; 3) PHR systems should support data interoperability. The relation and differences between EHR and PHR systems are defined and explained in detail in the ISO standard ISO/TR 14292:2012 [5].

The health Internet of Things (h-IoT) spans various kinds of health sensing technologies like medical IoTs, wireless health monitoring, and wearable sensors which are used to improve individuals' well-being. According to [6], the new sensing taxonomy of mobile health sensors is based on the purpose of these sensing technologies. It distinguishes 1) health and well-being sensors, 2) diagnosis sensors, 3) prognostics sensors, 4) assistive sensors. In this context, h-IoT devices are pivotal sources of data for EHRs and PHRs. The volume of health-related (big) data is rapidly increasing due to the increasing adoption of medical IoT devices. This trend demands developing a safe and compliant concrete framework and architecture to utilize this data treasure [6]. Big health data analytics can play a key role in improving individuals' well-being.

Due to the inherently distributed nature of how personal health data arises and is stored, data interoperability is a vital precondition for building useful PHR systems. Interoperability is the ability of different systems and applications to communicate and exchange data [6]. Interoperability can be legal, organizational, semantic, and technical. There are several common interoperability standards in the health domain. openEHR [7] provides a complete approach to develop compatible health systems, which as a result eliminates data interoperability issues. HL7/FHIR [8] are health data exchange standards for existing systems. ISO 13606 [9] is the European standard concerning data interoperability between EHRs. These and other more specialized standards ease the process of exchanging data between EHRs. Other interoperability standards like IEEE

11073 [10] concerning personal health devices (PHDs) become relevant for PHRs too because they concern interoperability embedded with medical IoT devices.

Decentralized ledger technologies such as blockchain and decentralized peer-to-peer techniques like the InterPlanetary File System (IPFS)[1] are together proving suitable to build solutions that exchange data between system stakeholders preserving data interoperability and data privacy. Thanks to cryptographic mechanisms, blockchain technologies provide decentralization, immutability, transparency, anonymity, and have emerged as promising solutions to data privacy-preserving management of data [11].

In this paper, we investigate the contemporary PHR systems, concentrating on merging and utilizing IoT data in PHR systems, and preserving patients' privacy in a data interoperable manner. The contributions include 1) leveraging data interoperability between EHRs and PHRs in data privacy enabled manner, 2) keeping patient data up to date by merging medical IoT data into PHRs, 3) facilitating big health data, and 4) developing a suitable safe, and secure data access management scheme based on blockchain and smart contracts.

In the following, Section II addresses the background and related work, Section III introduces the proposed IoT-based PHRs framework, Section IV explains the design of the EHW and Section V addresses the conclusions and future work.

II. Background and Related Work

A. Data Privacy and Interoperability using GDPR and FHIR

Data protection regulation is put in place to ensure the data privacy of data owners. Considering patients' privacy is vital when building information systems that provide digital services to patients. The new amendment of GDPR, the European regulation act that came into force in 2018, ensures the privacy of patients' data [12]. Patient's data privacy in e-Health should be managed along the entire data lifecycle: from the initial gathering, e.g., from medical sensors to their subsequent retrieving from PHR systems.

GDPR mandates the following eight rights for any citizen, including patients: 1) The right to access their data, 2) The right to delete their data, 3) The right to move their data, 4)The right to be notified when gathering their data, 5) The right to update their data, 6) The right to limit who can use data, 7) The right to be informed within 72 hours when their data is breached, 8) The right to stop the use of their data for marketing.

GDPR also insists on the right to data portability. In the PHR systems context, this means that data interoperability should be ensured (data export) and supported (data import) by health service providers. According to [3], the right of data to be portable is stated in the new 2018 amendment of GDPR. Concretely, to grant this right to the data owner (in our case, the patient) a user-centered data access system must be provided.

[1]https://ipfs.io/

A way to achieve these goals and comply with GDPR is to systematically adopt techniques like the Fast Healthcare Interoperability Resources (FHIR) [8] as a basis of the PHR system. The FHIR specification is a standard promoted by the HL7 organization for exchanging healthcare information electronically. It supports semantic data interoperability to ensure that data can be readable and interoperable when exchanging medical data between system stakeholders. HL7/FHIR uses Application Programming interfaces (APIs) to implement data interoperability when exchanging data from different data sources [8]. The semantic interoperability is due if all the system components refer to and implement the data types, messages, and protocols described in the HL7 standards. These standards can also help minimize the time and cost of translating from one format or language to another [13], because they serve essentially as a domain-specific language and reference for the health care domain. In our work, we adopt FHIR and HL7 compliance in the data and protocol layers.

B. Blockchain and Smart Contracts

Blockchain (BC) is defined in [14] as "*a distributed database of records*". Its first application was bitcoin, a cryptocurrency started in 2008 by a group that identifies as Satoshi Nakamoto. By using a cryptographic proof mechanism, BC eliminates the need to rely on third-party intermediaries when transferring money from one party to another. Thanks to general-purpose platforms like Ethereum and Hyperledger Fabric, since 2016 industries and researchers adopted BC well beyond the financial domain. While a permissioned BC allows only participants to see its transactions, a permissionless BC is public and any participant in the BC network can see transactions. BC caught the attention of developers and researchers in the healthcare sector. It is meanwhile applied to data management, data interoperability, monitoring systems, health supply chain management, and other areas. As our research focuses on data management, permissioned blockchain is according to Braunstein [8] the most suitable choice for EHR and PHR data management systems.

A smart contract (SC) is defined as a programmable contract that involves rules that need to be properly applied to do actions. An SC is essentially an orchestration or choreography of workflows on top of a BC. Given a BC of choice, a smart contract is programmed in the programming languages supported by that BC technology and it is deployed in the BC network. SCs and BC technologies will be used in our framework to allow the data owner (i.e. a patient) to define and apply access control rules to limit access privileges by medical service stakeholders (e.g. patient, medical service providers, and third parties). This is along the lines of [11].

C. Related Work

Several literature review articles on PHRs investigate privacy concerns and the application of BC in PHR systems. [15] analyses privacy and security issues of PHR systems and show that the compliance to data privacy regulations is low

in existing PHR systems. [16] investigates the suitability of blockchain for PHR systems. It concludes that BC could be useful to exchange data; however, cost, data size, and data privacy need to be considered while choosing such a solution. They emphasized that some BC technologies are public, and might not be suitable for sensitive systems like PHRs. Also, PHRs involve different kinds of data,e.g scan images which need suitable storage and network technologies.

Many studies try to solve data privacy issues through data management systems for PHR in an interoperable data manner. The OmniPHR architecture [17] integrates patient's data from EHR and PHR based on blockchain. It addresses the issues of distributed EHRs and data interoperability facilitation, but it does not comply with GDPR. [18] proposed to integrate personal health records based on the Modex BC database and provides a proof of concept of the approach. However, it is still a work in progress and the solution does not cover GDPR individual rights technically. Also, third parties are given limited time to access data without describing how that can be technically managed.

Other researches are limited to the data management aspect in PHR and do not cover data interoperability, which is a key point in PHR systems. The emergency access control data management system for personal health records in [19], based on blockchain and smart contracts, gives the control of accessing data to patients by limiting access to their data in emergency cases. Although patients can this way exercise some control to accessing their data, this solution does not cover all kinds of data and all situations. The personal data management approach in [20] complies with GDPR, but it does not cover the data interoperability aspect. The framework in [11] uses attribute-based encryption (ABE) technology to provide a fine-grained access control management based on users' attributes. It allows the data owner to control access to their data, however, also this study does not cover the data interoperability aspect of PHRs.

In conclusion, the need to consider at the same time access control and interoperability is still not solved, yet it needs to be addressed for PHR systems to be useful.

III. Proposed IoT-based PHRs Framework

Our solution focuses on IoT-based PHRs. It proposes a reliable framework for building a concrete PHR system that has to harness medical IoTs at its core. Its structure, illustrated in Figure 1, puts health IoT system data as the core seed of the PHR system. A layered approach to data and component/subsystem management leads to a clear scope and responsibility at each layer. The aim is an easily controllable and manageable prolonged utilization of the produced data from EHRs and IoT devices, to coherently organize and manage health big data in a manner that preserves data privacy and leverages data interoperability.

The proposed framework has the following six layers:

- **Health IoT Devices layer**: the devices are at the framework core, as they are the paramount sources of personal health data. Various kinds of health IoT devices are used to enhance patient's well-being. The massive amounts of health data they produce should be utilized efficiently.
- **Privacy Layer**: it involves all privacy standards related to the IT services offered to users and healthcare service for patients. GDPR, HIPAA, and other relevant privacy regulations must be considered from the inception when developing any personal health record system.
- **Data Management Layer**: a solid data management system entails data privacy and security techniques while allowing sharing data with other stakeholders. Encryption and anonymization technologies are addressed and developed in this layer, considering data protection regulations.
- **Data Interoperability layer**: it enforces appropriate interoperability standards - in our case the FHIR interoperability standards. This ensures the ability to exchange data between different systems, IoTs and EHRs, in a simple and understandable approach that saves costs and time.
- **Big Health Data layer**: it contains the big data and data analysis technologies and tools used to the ultimate benefit of using health data. Reliable personal health record systems should be able to utilize the mass data produced from health IoT devices.
- The **Health Services and Stakeholders** are the beneficiaries from the whole system framework. Here we include the patients, physicians, other healthcare providers, as well as other parties like research centers, and private companies which work in the healthcare field.

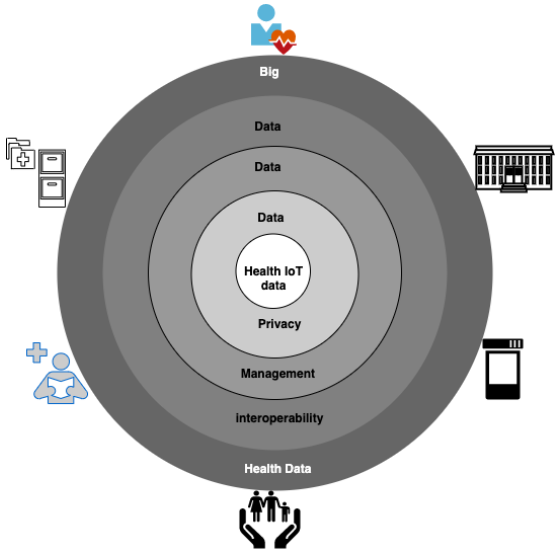

Fig. 1. The layered framework for a reliable IoT-based PHR

IV. EHW Design

We present an overview of the electronic health wallet (EHW) application architecture, followed by considerations about the application, data interoperability, data repository, and data sharing and management layers. Moreover, we briefly describe the future system features and prototype.

A. General Architecture Overview

The Electronic Health Wallet (EHW) is a PHR mobile application based on BC and FHIR, which are standards used to exchange data between patients' data sources, i.e. the IoT sensors and EHRs from different health care providers. EHW is an application for patients. It allows them to access their up-to-date health data which come from different systems. At all layers, APIs should be co-developed while developing the EHW app. Nonfunctional properties such as data privacy, security, interoperability, and performance are considered at the appropriate level of the IoT-based PHR framework. Figure 2 shows the high-level system architecture.

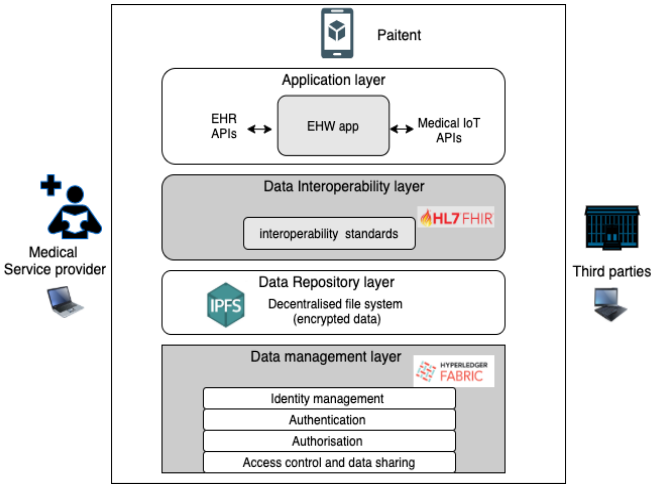

Fig. 2. EHW: High-Level Architecture

B. EHW Layers

At the **Data Management layer** we consider three main sources for PHRs data: EHRs, IoT data, and data provided by patients. EHRs potentially involve all the patient data history in the health organizations they visit. Also, data is produced by health and well-being sensors, diagnostic sensors, prognostic sensors, and assertive sensors, and maybe contributed to the PHR and the EHW app. Patients themselves should be able to enter further data into the PHR. For example, data measured by themselves, like their weight, blood pressure, temperature, etc., but also data linked from various fitness and well-being Apps. The data management system will cover identity management, authentication, authorization, and access control, effectively managing access and sharing rights to patient's data in the PHR system. A PHR system has three main stakeholder groups:

- The **patients** are the data owners, who should control all access requests to their data according to GDPR, e.g. when requests come in an informed consent context.
- The **service providers** should be able to access and add data to the PHR following the granted permissions. They should also be able to update those permissions as needed, by terminating some access rights and asking for new permissions as needed.
- **Third parties** may seek special-purpose access to patient data. For example, a research center may ask to include a patient's data in studies for scientific purposes, or a repository may seek to collect data e.g. for conservation purposes (like a rare diseases registry).

Blockchain technology plays two roles in this system: to provide a unified history record for patient' data (i.e. PHR) and also as an authentication, authorization, entity management, and access control server to access data in an IPFS distributed peer-to-peer file system. Smart contracts (SC) are used to allow patients to control their data, as a truly patient-centered system. This happens in our system by providing a fine-grained access control based on user identities and attributes. Using blockchain and smart contracts, the access rules will be enforced on whoever requests data from IPFS. Four main functions in the SC will allow patients to control the data access: AddPolicy, UpdatePolicy, HashPolicy, and AccessPolicy. The IncentivePolicy function provides incentives to patients to share their data with third parties based on a trade-off philosophy, to encourage them to support big health data when they agree to share. Sharing may positively impact their well-being, as described in [21].

Data management and sharing techniques ensure that patients are allowed to control their data and ensure their right to share data with whom they wish. Patients will be encouraged to share their data with stakeholders (e.g. research centers, but also service providers, insurances) on an informed consent-based basis. The attractiveness of sharing will be connected to enabling a better individual service (based on more accurate or complete information), but also enhanced services, based on the ability to use or access information and services that use the collectively shared big data, with a potentially positive impact on the individuals' well-being. Thus, the sharing opportunity and technology are proposed as a part of the data management, as an incentive for patients to share data while preserving their privacy.

The **Data Repository layer** is decentralized, as the data may reside in distributed locations. IPFS presents a new platform for writing and deploying applications and a new system for distributing and versioning large data. The OAuth02.o and OpenID protocols are used to ascertain authentication and authorization while exchanging data between data sources. Data will be stored and encrypted in IPFS so that any stakeholder can access it by deploying smart contracts in the blockchain network. The patient, as the data owner, manages the data access control to the own data by granting and revoking privileges to parties who seek access to that data.

In the **Data Interoperability layer** we adopt the Fast Healthcare Interoperability Resources (FHIR) standards. They are commonly applied in healthcare data interoperability for their suitability and flexibility. To ensure compliance with European health regulations, our system considers also ISO 13606, the European EHR data interoperability standard. The FHIR standard allows a good level of semantic data interoperability, as it is based on domain-specific standardized application programming interfaces (APIs) and standardized complex

data types. These data structures and APIs will be the medium of choice to post and get data (in XML or JSON format) to exchange medical data between various stakeholders and data sources. The Hyperledger fabric blockchain or another suitable blockchain technology is going to be used to work as a platform to allow data interoperability.

The **Application layer** will be a web or mobile application. The EHW App will allow patients to be up to date with their health data, presented as a unified record. The Health data provided by EHW may involve diagnostic reports, treatment plans, and personal health IoT information.

C. System Features and Prototype

The target features of the PHR system and EHW application are summarized in Table I, showing the central requirements for the PHR framework, the solution characteristics (top-level features), and the top benefits of the privacy technique.

IoT-based PHRs framework leverages:	Solution characteristics:	A privacy-preserving technique supports:
• Reliability • Scalability • Data privacy • Data interoperability • Health big data	• A holistic privacy preserving approach • Based on decentralised system • Reliable architecture • Patient-centred system	• Anonymity • Data tamper-proof • Access control • Encrypted data

TABLE I
PHR SYSTEM FEATURES

A prototype for the system is going to be built using a low-code model driven design (MDD) approach based on the eXtreme Model-Driven Development (XMDD) paradigm [22] [23]. The DIME Integrated Modelling Environment is used for the design, validation, implementation, and deployment of the system [24].

V. CONCLUSIONS AND FUTURE WORK

The main concept of PHRs is to enable patients to access their data real-time anytime and to share it with whom they wish. This should happen in an interoperable and privacy-enabled manner. We described a framework for IoT-based PHR, considering IoT as a paramount data source to PHR. We also introduced the EHW PHR application architecture and explained how it uses blockchain, IPFS, and FHIR' APIs to deliver data privacy and data interoperability. In the next step, we are going to implement the architecture and framework in a model-driven way, using a low-code integrated modeling environment to design and implement the system in an agile way. The system will incentivize data sharing, technically implemented with fine-grained access control using Hyperledger Fabric blockchain technologies. The solution performance will be evaluated with Hyperledger caliper. The selected case study concerns chronic disease patients within the Limerick Health Research Institute network of collaboration.

ACKNOWLEDGEMENTS

This work was supported, in part, by Science Foundation Ireland grant 13/RC/2094 to Lero, the SFI Research Centre on Software (www.lero.ie). It was also supported in part by ALECS, the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 754489.

REFERENCES

[1] "Health Information Privacy: Summary of the HIPAA Security Rule." [Online]. Available: https://www.hhs.gov/hipaa/index.html
[2] "GDPR.EU:Complete guide to GDPR compliance." [Online]. Available: https://gdpr.eu/
[3] P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, and I. Sanchez, "The right to data portability in the gdpr: Towards user-centric interoperability of digital services," *Computer Law Security Review*, vol. 34, pp. 193–203, 2018.
[4] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, "Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption," *JAMIA*, vol. 13, pp. 121–126, 2006.
[5] "ISO/TR 14292:2012, Health informatics — Personal health records." [Online]. Available: https://shop.standards.ie/en-ie/standards/iso-tr-14292-2012-599846_saig_iso_iso_1373468/
[6] R. S. Istepanian and B. Woodward, *M-health: Fundamentals and Applications*. John Wiley & Sons, 2016.
[7] "openEHR:Open industry specifications, models and software for e-health." [Online]. Available: https://www.openehr.org/about/what_is_openehr
[8] M. L. Braunstein, *Health Informatics on FHIR: How HL7's New API is Transforming Healthcare*. Springer, 2018.
[9] "Iso13606." [Online]. Available: http://www.en13606.org/information.html
[10] "ISO/IEEE 11073 Health informatics — Personal health device communication." [Online]. Available: https://www.iso.org/standard/61897.html
[11] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38 437–38 450, 2018.
[12] "European commission (2020). 'eu data protection rules'." [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection
[13] T. Benson and G. Grieve, *Principles of Health Interoperability*. Springer, 2016.
[14] S. Underwood, "Blockchain beyond bitcoin," *Communications of the ACM*, vol. 59, pp. 15–17, 2016.
[15] J. L. F.-A. I. Carrión Señor and A. Toval, "Are personal health records safe? a review of free web-accessible personal health record privacy policies," *Journal of medical Internet research*, vol. 14, p. 114, 2012.
[16] Y. R. Park, E. Lee, W. Na, S. Park, Y. Lee, and J.-H. Lee, "Is blockchain technology suitable for managing personal health records? mixed-methods study to test feasibility," *J Med Internet Res*, vol. 21, p. e12533, 2019.
[17] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "Omniphr: A distributed architecture model to integrate personal health records," *Journal of Biomedical Informatics*, vol. 71, pp. 70–81, 2017.
[18] A. Cernian, B. Tiganoaia, I. Sacala, A. Pavel, and A. Iftemi, "Patient-datachain: A blockchain-based approach to integrate personal health records," *Sensors*, vol. 20, p. 6538, Nov 2020.
[19] A. R. Rajput, Q. Li, M. Taleby Ahvanooey, and I. Masood, "Eacms: Emergency access control management system for personal health record based on blockchain," *IEEE Access*, vol. 7, pp. 84 304–84 317, 2019.
[20] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "Gdpr-compliant personal data management: A blockchain-based solution," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1746–1761, 2020.
[21] B. Alamri, I. T. Javed, and T. Margaria, "Preserving patients' privacy in medical iot using blockchain," in *Edge Computing*. Springer, 2020, pp. 103–110.
[22] T. Margaria and B. Steffen, "Agile it: Thinking in user-centric models," in *ASoLA*. Springer Berlin Heidelberg, 2008, pp. 490–502.
[23] ——, *Service-Orientation: Conquering Complexity with XMDD*. Springer London, 2012, pp. 217–236.
[24] S. Boßelmann, M. Frohme, D. Kopetzki, M. Lybecait, S. Naujokat, J. Neubauer, D. Wirkner, P. Zweihoff, and B. Steffen, "Dime: A programming-less modeling environment for web applications," in *ASoLA*. Springer, 2016, pp. 809–832.