Considering Ethics in Model View Controller Architectures in Human Computer Interaction Health Domain

Ulrich Kowohl
FernUniversität in Hagen
Faculty for Multimedia and Computer Science
Hagen, Germany
Ulrich.Kowohl@fernuni-hagen.de

Felix Engel
Research Institute for Telecommunication and Cooperation
Dortmund, Germany
fengel@ftk.de

Raymond Bond
Ulster University, N. Ireland
School of Computing
rb.bond@ulster.ac.uk

Maurice Mulvenna
Ulster University, N. Ireland
School of Computing
md.mulvenna@ulster.ac.uk

Matthias Hemmje
Research Institute for Telecommunication and Cooperation
Dortmund, Germany
mhemmje@ftk.de

Ethics in digital resource processing and access are strongly coupled with human computer interaction because they produce trust between user and system. Over the past decades, we have seen a rapid increase of digital born resources in business applications where i.e. different stakeholders, ranging from patients, doctors to Data Scientists must cope with ethical aspects and regulations. Amongst others, innovative Model View Controller (MVC) based data management systems in the healthcare sector are analysing and managing an ever-growing, vast amount of sensitive data, enabling its efficient and comprehensive use in decision-making processes. E.g. in data-driven collaboration processes like drug development, caregiving or clinical patient monitoring. MVC is one of the most popular architectural patterns (Holzinger et.al 2010), which is the reason to investigate this design pattern further in terms of ethical aspects within human computer intractable systems. However, new regulations, like the GDPR have a huge impact on sensitive data management. However, ethical regulations could not first be considered by those who make use of information system functionalities, but must be an inherent part of considerations during software development process. This short paper will bring up and discuss ethical issues in decision making systems system software development, along with an existing ethic by design framework in the scope of health-related research projects.

Ethics, Data Sharing, Architecture.

1. INTRODUCTION

Communication is essential within medical treatment. Communication issues and bad teamwork are e.g. responsible for over 30% of incidents within clinical care (Suresh et. al 2005, Pronovost et. al 2016). Greenberg has analysed 444 incident cases and proved that 14% of those cases are related to issues within teamwork and communication within team members (Greenberg et. al 2007). In other words: Within medical processes it is important that each team member knows at each time all information he has to know to be able to fulfil his or her task. Within this paper we are going to present a system architecture concept in order to be able to tackle human communication issues within decision making systems system in health applications, with a focus on data management driven collaboration and process management. Further, we will outline an evaluation approach when it comes to ethical issues within sharing information across medical teams and their related computer human interactions. Historically healthcare organizations did not have a comprehensive view of operational processes and information, which means that no participant had an exact overview of all existing information within the process. It is recommended to treat data as strategic asset and put process and systems in place to access and analyse the right data to inform decision making processes and drive actionable results (IBM 2015)] and steer processes, which is highly interrelated with data sharing between stakeholders. For this, data has to comply with certain ethical standards. (Herschel et. al 2017)] This paper visits a subset of medical processes and aligns them in a high-level software architecture and outlines an ethical value framework for evaluating the system and its underlying human computer interactions afterwards.

Therefore, we will first introduce three different categories of research fields and their processes and align them among ethical regulatory rule sets.Those rules will form a short set of requirements building the design principles of a software architecture in order to fullfil the needs of a good computer human interactable data management system for medical domains capable of driving medical processes based on its data.

2. APPLICATION DOMAIN

SenseCare (Sensor Enabled Affective Computing for Enhancing Medical Care) is an EC co funded project, to provide a platform for software services in dementia care to assist medical professionals, care givers and patients to ease processes by sharing information across the stakeholder domains for home caring. It will integrate data from multiple sensors to support emotional insight, well-being and cognitive state for stakeholder collaboration among certain processes (Kowohl et. al 2017). Therefore, data needs to be archived in searchable accessible and interpretable way. Goal is, that gathered information enables stakeholders to provide better medical treatment and diagnostic results. Personal Drug Development (PDD) on the other side is another opportunity to seize an opportunity in the area of personalized molecular cancer diagnostic assay development. Delivering the right person, right time, right treatment compelling. The development of new diagnostic tests for use in a clinical setting entails two key phases namely (i) assay development (AD) and (ii) clinical validation (CD) distributed among different stakeholders. AD is about generating large data sets and knowledge discovery (KD). The quality of knowledge discovery will be then determined within the CD phase. Last but not least, the novel **Immunology Monitoring** (IM) opportunity tackles areas of carrying out targeted, hypothesis driven studies for clinical care by microbiome profiling with electronic health records interlinking for developing biomarkers allowing clinicians to maximize quality of clinical monitoring.

Introduced research fields yield different objectives, but are aiming for human intractable computer systems designed for orchestrating processes by sharing information in order to provide the right information to the right user at the right time enabling them to carry out their work properly. Although when it comes to information sharing between users of a system, there are quite a few ethical regulations on data protection.

3. COMPUTER INTERACTION ETHICS WITHIN MEDICAL DOMAIN

The obligatory General Data Protection Regulation (GDPR), tackles data security and privacy concerns. GDPR introduces Privacy by Design (PBD) as rule of play (fatml 2016) assessed by audits. Security will be introduced as dedicated stakeholder and should be independent of human risk factors e.g. misconfigurations. Auditable standards and technologies are preferred as well as there should be no trade-offs between functional and security requirements given. Data collection, disclosure, retention and usage has to be defined and limited to a purpose defined upfront. Collected data and information has to be kept to a minimum and applied to infrastructure e.g. logging as well. The system has to be user centric, user interactions have to be traceable in order to keep transparency while – at the same time – metadata of user activity underlies the same GDPR rules other data. Over the complete lifecycle of data existing within the system, it has to be correct and complete related to purpose. This accuracy has to be maintained even for failure cases. (De Hert et.al 2012)

Ensuring technologies are ‘ethical-by-design’ (Mulvenna et. al 2017) is imperative if we are to proceed into a society that is concerned about preserving a high standard of morals and integrity. Technology today often use persuasive design and nudge theory to encourage users to take impulsive actions. This has been called ‘evil by design’ and ‘dark patterns’. Ethical guidelines in the area of computer ethics have been proposed in many sub-disciplines, including user experience design (De Hert et.al 2012)]. Hence, it is important to provide ethical guidelines to support the building and auditing of algorithms, architecture and other data science practices. Mulvenna et al. have started to compile ethical-by-design principles applying as well on human intractable computer systems. They aim on supporting people using the product or service by engendering empathy for users. The System has to empower the user to take informed decisions by providing enough information, the user has to be able to choose when and how he engages with the services. The system has to be customizable in order to adopt to user needs. The system should be able to support shared decision making as well as failure handling, transparency and reporting if necessary. These initiatives have disseminated the need for ethics in data science and technology, but we may realise that specific guidelines for ‘health data science’ will be more impactful, after all, health data is very sensitive and today we would need to start with making health data available to the individual, hence ‘any data about me should be accessible to me’ – however this is complicated as arguably some data is harmful to patients. This leads into the need of a generic platform ecosystem providing services in order to empower users to configure their own collaborative data management systems. Therefore, following requirements can be stated for the architecture:

Should at least provide services specialized to the users and client needs, within a platform approach:

- support multiple tenants (Req 1)

- Data has to be collectable so that it can be managed and used among the medical processes (Req 2)
- Should guide user groups through their dedicated processes (Req 3)
- Should give users the chance to do informed decisions (Req 4)
- Should give users exactly that information they need, not more (Req 5)
- Should store data in a way that processes and results are transparent and repeatable (Req 6)
- Should store information for retention and not go beyond its periods (Req 7)

4. COMPUTER INTERACTION ETHICS WITHIN MEDICAL DOMAIN

Following (Kowohl et. al 2017), a configurable user empowering system architecture would result into following basic principles: (1) The user is free to choose which services of a data management platform (DMP) he will use. (2) Basic functions of the platform are configurable and generic enough so that can be used for users use cases (3) DMP services support separate tenants having different configurations serving the tenants different use cases (Req 1). Following MVC as one of the standard architectural principles (Holzinger et. al 2010, Rosa et. al 2015), we can divide the platform into different layers: Presentation layers (View), facilitation layers (Controller), service layers and persistence layers (Model). We choose MVC as foundational architectural pattern because MVC provides multiple “views” which can be considered as different clients or tenant implementations which references to (Req 1). We introduced three different projects from different medical domains: Home care giving, Clinical care and monitoring as well as scientific research in personalized drug development. Within the DMP those use cases would be placed on top of the data management platform, so that we can identify for each tenant a dedicated tenant use case module making use of the DMP. Therefore, the DMP has to provide specific services: A Data import component has to be existing, loading and enriching data with enough information in order to be able to be presented to the user (Req 2).This import component forms a pipeline of several configurable steps. Raw data has to be gathered and enriched by meta- information as well as feature data. Meta-Information is the part of information about raw data which is stable and – in case of e.g. sensory data – does not change over time. Feature data is directly interconnected with raw data and changes over time e.g. emotion expressions within videos. Those data import components have to be configurable and extendable for the clients itself, since pipeline configuration as well as feature and meta information extractions highly depends on the tenants needs. The data should not directly be available for each user, since each user should have at each step in his own process flow exactly the data available he needs. Therefore, the system has to be able to understand the working model of the users and engage them within a processes

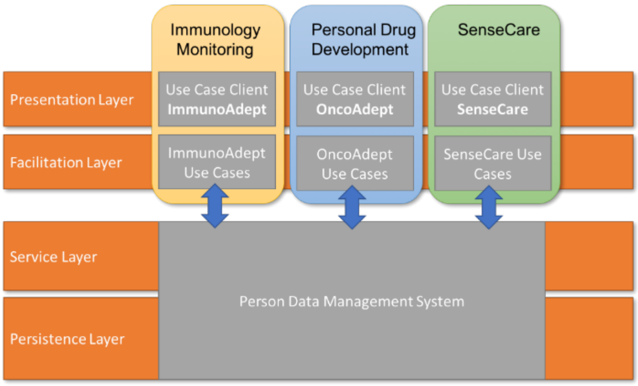

Figure 3: Use Case API Modules

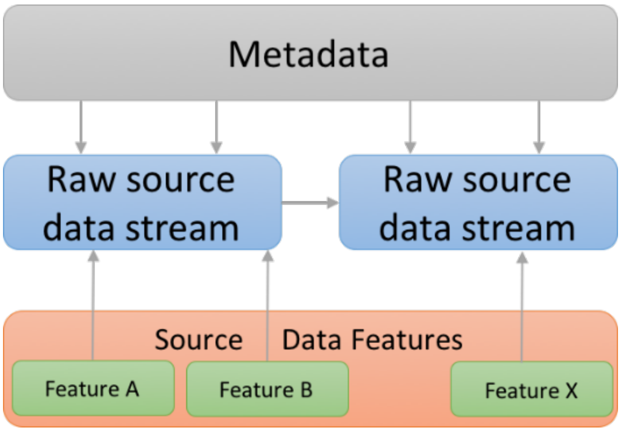

Figure 1: Data Structure

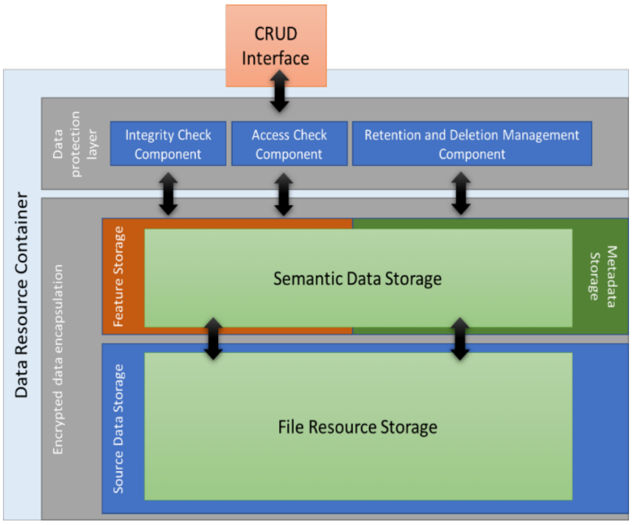

Figure 2: Data Store

workflow, which has to be managed within a dedicated workflow component (Req 3). A workflow can thereby be considered as a graph (K,V) K being tasks and V = K x K transitions between tasks. Each Task has a defined target (the user who has to solve the task) as well as an entry data set and a final data set. The entry data set is the data presented to the user in order to make informed decisions (Req 4 and Req5). Solving a task adds additional data to the entry set, so that the final set can be defined as entry set + data which has been added or linked to the task. (Req 5 and 6) are aiming on data security within storing data. (Req 5) defines a security dimension on data, so that data will be visible only to the right person at the right time. Data security will not be static anymore, it will be embedded within a process context and adds state full behaviour on data security components since e.g. the user should not see specific data after solving a dedicated task. While data as well has to be secured and be consistent according to GDPR, which should be managed by a data security component. Managed data (metadata, raw and feature data) is inter-linked using semantic and raw (e.g. file or database) storage. GDPR aims on valid data sets which makes storage of data challenging within retention deletion processes. Therefore, data has to be stored in a universal transactional storage fulfilling storage and GDPR related tasks like consistency checks and retention management. GDPR enforces data sets to be correct and complete (Req 7) within their retention periods. After retention invalidates, data has to be deleted immediately. (Kowohl et. al 2017) has shown, that error cases in deletion processes can lead into incomplete or outdated data. To compete this, an entirely new storage structure will be applied as shown in Figure 3. Data Access, integrity checks and retention/deletion management will be carried out by the data entity itself in order to form an atomic unit defined as smallest logical piece of information. Therefore, information objects will consist of different storage types as well as functional components to keep GDPR compliance.

4.CONCLUSION

Within this paper we outlined ethical regulations, issues and introduced requirements and a a general architecturual MVC based frameworks for computer human intractable systems in the domain of medical data management and data management process orchestration. We presented a novel architecture in order to tackle the current regulations as well as being compliant to the ethical manifesto presented in (Mulvenna et. al 2017). We outlined the need for configurable components as well as the need for an entirely new data storage concept for process oriented medical data. It will be the task for future work to implement the presented architecture among its functional requirements and needs in order to verify the correctness of the presented architectural approach.

5. ACKNOWLEDGMENT

This publication has been produced in the context of the SenseCare project. The projects have received funding from the European Union's Horizon 2020 program under grant agreement No 690862. However, this paper reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

6. REFERENCES

Reevse, C., Badnar D. (1994) Defining Quality: Alternatives and Implications, ACAD Manage Rev, Vol 19, 419 – 445

International Business Machines Corp., (2015) Data Driven Healthcare Organizations use big data analytics for bit data gains, https://www-03.ibm.com/industries/ca/en/healthcare/documents/Data_driven_healthcare_organizations_use_big_data_analytics_for_big_gains.pdf (2018/03/15)

Herschel R., Miori V (2017. Ethics & Big Data, Technology in Society, Vol 49, 31-36

Casado M., Garfinkel T. (2008) Sane: A Protection Architecture for Enterprise Networks, Usenix Security Symposium, July 31st 2008, 137-151

Mulvenna, M, Boger, J., Bond, R. (2017) *Ethical by Design - A Manifesto.* In: European Conference on Cognitive Ergonomics 2017 (ECCE 2017), Umeå, Sweden. ACM Digital Library

O'Neill, C., (2016) Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Allen Lane, 272 pages

Kowohl, U., Engel, F., Dassler P., Hemme M.: Case Study: Management of Affective Data and Data Fusion in eHealth Appliances under Consideration of Legal Frameworks. CERC 2017, ISSN 2220-4164, pp 200 – 208

Evil by Design, http://evilbydesign.info, 2018/06/03

Dark Patterns, https://darkpatterns.org, 2018/09/03

UXPA, http://www.uxpa.org/resources/uxpa-code-professional-conduct, 2018/6/03

De Hert, P., Papakonstantinou, V. (2012). "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals". In: Computer Law & Security Review, 28(2), pp.130-142

FAT/ML (2016) Fairness, Accountability, and Transparency in Machine Learning, http://www.fatml.org, Accessed 28 February 2017

Suresh G., Horbar J.D., Pisek P., Gray J., Edwards W., Shiono P., Ursprung R., Nickerson J., Lucey J., Goldman D. (2005) Voluntary anonymous reporting of medical errors for neonatal intensive care, Pediatrics 2005, PubMed 15173481

Pronovost P., Berenholtz S., Goeschel C., Needham D., Sexton J., Thompson D., Lubomski L., Marsteller J., Markary M., Hunt E. (2006), Creating High Reliability in Health Care Organizations, Research 41, doi 10.1111/j.1475-6773.2006.00567.x

Holzinger A., Debevc M., Struggl K. (2010) Applying Model View Controller (MVC) in design and development of information systems: An example of smart assistive script breakdown in an e-Business application, e-Business (ICE-B)

Rosa J., Silva H., Matias R. (2015) A web based framework using a Model View Controller architecture for human motion analysis, Bioengineering (ENBENG), Porto 26.-28. Febr. 2015, IEEE