UNIVERSITY OF TARTU

Faculty of Science and Technology

Institute of Computer Science

Sanam Nisar

Defining Blockchain-Based Techniques for Privacy Conflict-Resolution in Cross-Organizational Processes for E-Health Systems

Master's Thesis (24 ECTS)

Technical Supervisor: Aleksandr Kormiltsyn, MSc

Academic Supervisor(s): Alex Norta, PhD

Vimal Dwivedi, MSc

Tartu 2022

Defining Blockchain-Based Techniques for Privacy Conflict-Resolution in Cross-Organizational Processes for E-Health Systems

Abstract

Despite the great potential for healthcare professionals, individuals, and researchers, the integration of healthcare information from personal health records (PHR) and electronic health records (EHR) systems is complicated because of structural and semantic heterogeneity, trust, and privacy. Healthcare data is an emotional issue because of fear of privacy violations. Blockchain technology enables a patient's data privacy, transparency, and immutability in cross-organizational processes where a patient regulates access to his data and is aware of its usage. At the same time, blockchain technology creates new challenges for e-healthcare systems such as data privacy, observability, and online enforceability. In the thesis, we propose a design of a secure blockchain-based and patient-centric system with a definition of PHR requirements, an ontology for privacy-conflict resolution, and management mechanisms. Throughout this research, we illustrate our ideas with a running case about preventive and personalized healthcare.

CERCS: **T120 System technology, computer technology**

Keywords: Blockchain, Privacy Conflicts, Conflict Resolution, e-healthcare, PHR, EHR.

Plokiahelapõhiste Tehnikate Määratlemine Privaatsuskonfliktide Lahendamiseks Organisatsioonidevahelistes e-tervise Süsteemide Protsessides

Lühikokkuvõte: Hoolimata tervishoiutöötajate, üksikisikute ja teadlaste suurest potentsiaalist, on tervishoiuteabe integreerimine isiklikest tervisekaartidest (PHR) ja elektroonilistest tervisekaartidest (EHR) keeruline struktuurse ja semantilise heterogeensuse, usalduse ja privaatsuse tõttu. Tervishoiuandmete talletamine on emotsionaalne probleem, kuna kardetakse privaatsuse rikkumisi. Plokiahela tehnoloogia võimaldab patsiendi andmete privaatsust, läbipaistvust ja muutumatust organisatsiooniülestes protsessides, kus patsient reguleerib juurdepääsu oma andmetele ja on nende kasutamisest teadlik. Samal ajal tekitab plokiahela tehnoloogia e-tervishoiusüsteemidele uusi väljakutseid, nagu andmete privaatsus, jälgitavus ja veebipõhine jõustatavus. Lõputöös pakume välja turvalise plokiahelapõhise ja patsiendikeskse süsteemi koos PHR-nõuete määratlusega, ontoloogiaga privaatsuskonfliktide lahendamiseks ja haldusmehhanismide jaoks. Kogu selle uuringu käigus illustreerime oma ideid reaalse juhtumiga ennetava ja isikupärastatud tervishoiu kohta.

CERCS: **T120 Süsteemitehnoloogia, arvutitehnoloogia**

Võtmesõnad: Plokiahel, Privaatsuskonfliktid, Konfliktide Lahendamine, e-tervishoid, PHR, EHR.

List of Abbreviations and Terms

PHR	Personal Health Record
EHR	Electronic Health Record
GDPR	General Data Protection Regulation
OWL	Web Ontology Language
BPMN	Business Process Model and Notation
CPN	Colored Petri Nets
HIPPA	Health Insurance Portability and Accountability Act
AI	Artificial Intelligence
GMCR	Graph Model for Conflict Resolution
ADS	Algorithmic Decision-making System
HMMs	Hidden Markov Models
NFT	Non-Fungible Token
DAOs	Decentralized Autonomous Organizations
MAS	Multi-Agent Systems
AOM	Agent-Oriented Modelling

Table of Contents

List of Figures

List of Tables

1. Introduction

Over the past decade, blockchain has emerged as a key technology and attracted computer scientists and domain experts from different sectors. Blockchain has immense business potential in many applications, which has made it a hot topic among the stakeholders from different sectors including supply chain, food management, banking, and healthcare [1-3]. Healthcare and medical services are important and time-critical services that need to be delivered by secure and safer means at a required time [4]. Blockchain applications in the healthcare sector generally require string authentication, interoperability, data collection, and storage. Due to legal requirements, like the Health Insurance Portability and Accountability Act of 1996 (HIPAA) secure data collection and storage, and record sharing requirements are essential for blockchain-based applications [5].

Blockchain is a decentralized transaction and data management technology that provides security, anonymity, transparency, decentralization, traceability, and immutability [6]. These characteristics make blockchain technology useful for applications in healthcare. Blockchain is decentralized, there is no single authority for the decision making instead it uses a distributed network approach. It provides transparency by storing all the information within a blockchain transaction, which is publicly visible to everyone on the network. This not only provides transparency but also enables the traceability of transactions and data by their timestamp [6, 7]. Data in the blockchain is immutable, blockchain ledgers are persistent because of their ability to keep data unchanged and unaltered. Usage of blockchain improves the standards of interoperability while keeping the patients' records secure and confidential, which helps to provide patients privacy and control over their medical records. In the healthcare ecosystem, blockchain can improve data sharing and storing systems owing to its decentralization, immutability, transparency, and traceability features.

With time new technologies have emerged offering serval efficient ways to collect, process, and share medical health data. Health data is used for research purposes, to enable patients to manage their medical records and diseases. It also improves the efficiency, quality, and safety of healthcare systems. However, when it comes to security it raises new challenges related to data security and privacy. On 25th May 2018, European Union (EU) General Data Protection Regulation (GDPR) was established as the world's toughest privacy and security law passed to ensure safe and secure data collection, processing, and sharing of EU citizens. Any organization European Union (EU) or Non-European Union (non-EU) is obliged to follow GPD regulation when they aim or collect data on European citizens [8]. The Data Protection Regulation has defined principles for patients' data and these principles apply to all use of patients' data and all data controllers in healthcare systems. Article 5 contains all important principles, if any data controller neglects them then the data usage is not lawful. All the controllers must respect and follow the defined principles consisting of Fairness and transparency, Lawfulness, Accuracy, Integrity and confidentiality, limited Storage, Purpose limitation, data minimization, and Accountability [8].

Patients are a partner in the healthcare system, and their satisfaction and needs should be considered as a part of the system's quality definition. Recently, there have been many data breaches that exposed patients' financial and medical records. Existing healthcare systems are not able to provide enough security against data breaches but are also plagued by high costs [9] and the importance of the economic interests of healthcare providers [10]. For example, the privatization in the Irish hospital sector results in an increase in patient bed numbers in private for-profit (PFP) hospitals and a decrease in public- and private not-for-profit hospitals [10]. The existing system is not patient-centric, the patient is not the author and owner of his/her medical data, with less control over his medical record to share with other individuals, including healthcare professionals. As patient data privacy is the biggest concern when it comes to data sharing across different medical bodies, currently blockchain has been used in cloud computing with attribute bases encryption for secure sharing and scalability of Personal Health Records. It has enabled systems to be interoperable, data tamper-proof, and optimized medical services but it also brings privacy conflicts, architecture, and adoption challenges for integrated e-health systems.
Privacy conflict is a major challenge of the PHR system, this thesis' main goal is to create privacy resolution techniques and implementation of blockchain technology to create a prototype.

1.1 Problem Statement

Healthcare is an integral part of life. Unfortunately, the incessant aging of the population and the increase in chronic diseases place a significant burden on modern healthcare systems [11], and the demand for resources which include doctors, nurses, and hospital beds is high. The rapid development of the Internet of Things (IoT) paradigm has revolutionized the healthcare industry, bringing significant improvements in terms of e-health/medical records (EHR/EMR), prescription drug data, and insurance information.

However, the safe handling of EHR/EMR has become a very difficult task because the data is scattered across different medical institutions. Most existing healthcare systems are centralized and vulnerable to the single point of failure and information leakage due to the growing cyber-attacks [12]. The leakage of personal and critical information of patients can lead to serious consequences. In addition, modern medical systems do not provide transparency, reliable traceability, immutability, auditability, confidentiality, and security in the management of EHR/EMR.

In healthcare, the Internet of Things (IoT) offers many benefits, including the ability to better monitor patients and use data for analytics. When it comes to IoT for integrating medical devices, the focus is shifting towards consumers such as glucometers, blood pressure cuffs, and other devices designed to record patient vitals. This allows health care providers to automatically collect information and apply decision support rules to ensure earlier intervention in the treatment process.

Unfortunately, healthcare companies often do not consider the security risks of connecting these devices to the internet Patient-centric systems improve the efficiency and quality of healthcare

work. But the development of PHR/EHR has some problems inherent in them such as non-standard hospital management, poor standardization, and lack of interoperable software development. Every company uses its own designed standards for device manufacturing and data collection and storage which is also one of the major problems due to which, PHR/EHR is not able to share medical information in cross-organizational e-health processes.

Lack of formal evaluation of HR is another important issue and research [13] evaluated existing PHRs and states that PHRs have limited functionality. "The data entry, validation, and information display methods they employ may limit their utility as representations of medical information" [13]. A solution is needed to reduce the burden on health systems while continuing to provide high-quality care to at-risk patients [14].

Considering these problems in modern healthcare systems, blockchain technology can solve them [15] [5] [16] [17]. It is estimated that the implementation of the blockchain could lead to savings of up to $100–150 billion per year by 2025 in the costs associated with data leakage, as well as by reducing the incidence of fraud and counterfeit products [18]. Blockchain is a promising technology that can help streamline healthcare data management operations, enabling unprecedented data efficiency and trust-building [19] [20] [21] [22] [23] [24]. It offers a variety of important and built-in features such as transparency, decentralized storage, data access flexibility, secure authentication, immutability, interconnection, and security, which allows the extensive use of blockchain technology for healthcare data management [25] [26].

1.2 Objectives and Roadmap

1.2.1 Research Objective

This research aims to identify important privacy conflicts in the e-health cross-organizational process and develop a block-chain based prototype for the resolution of conflicts. The main objectives are:

1. Analyze existing privacy issues and their solutions
2. Describe how a PHR integrated into EHR results in security, privacy, and privity conflicts.
3. Proposing privacy resolution techniques for cross-organizational process in an e-health system
4. Develop a block-chain based prototype, implementing privacy resolution techniques.

1.2.2 Research Questions

Healthcare data is an emotional issue because of fear of privacy violations. Blockchain technology enables a patient's data privacy, transparency, and immutability in cross-organizational processes where a patient regulates access to his data and is aware of its usage. At the same time, blockchain technology creates new challenges for e-healthcare systems such as data privacy, observability, and online enforceability. In this research, we propose a design of a secure blockchain-based and patient-centric system with a definition of PHR requirements, an ontology for privacy-conflict

resolution- and management mechanisms. Using defined privacy conflict resolution techniques, a prototype will be developed using block-chain based smart contracts.

RQ: How to define blockchain-based techniques for privacy conflict-resolution in cross-organizational processes for e-health systems?

The main question is divided into three different how questions which address the identification of vital cross-organizational processes, how to resolve the privacy conflicts of identified processes, and mapping privacy resolution techniques to e-health systems. Following are the sub-questions:

- SRQ1: How to identify privacy conflicts in the e-health cross-organizational processes?
- SRQ2: How to resolve privacy conflicts in e-health cross-organizational processes?
- SRQ3: How to map privacy resolution techniques to decentralized e-health systems?

These three sub-questions are formulated in sequential order according to their importance e.g. First sub-research question is about identification which is the first step to identifying the conflict before you design a resolution technique.

SRQ1: Identification of important processes in the e-health cross-organization process is the first step. In this step, selection for specific processes will be made from the list of all processes. For selecting a process, we need to identify the processes which have patient privacy conflicts. Basic requirements will be defined as a checklist for process selection. Following are further three sub what questions that address the selection of important processes, setting up the requirements for selecting a process and marking it as important, and then using the selected processes to check the privacy conflicts related to them:

- What are important e-health cross-organizational processes?
- What are the requirements for privacy conflict identification in the e-health cross-organizational processes?
- What are privacy conflicts in e-health cross-organizational processes?

SRQ2: Once process selection from research question one is done, the next step is the resolution of conflicts for e-health cross-organizational processes. Before designing the resolution techniques, it is important to analyze existing techniques. Finding the issues and gaps in current techniques is important before designing new techniques, this approach will cover more conflicts and help to achieve higher quality. Resolution of privacy conflicts does not only include finding existing techniques which are being used but also selecting how many of them are decentralized and then setting up the criteria why to select a technique for implementation. Following are the two sub-questions that help with the conflict resolution step:

- What are the existing decentralized privacy conflict-resolution techniques for e-health cross-organizational processes?
- What are the criteria for the decentralized privacy-conflicts resolution techniques?

SRQ3: Moving to the Third research question which covers mapping of identified/newly designed techniques to decentralized systems. Before mapping resolution techniques, it is important to understand and design the system architecture. It is a vital part, to understand and design all the important components of the system before moving to the next step. Technology stack selection comes as the last step before the implementation of the prototype. Following are two sub-questions:

- What is the architecture for a decentralized e-health privacy-conflict resolution system?
- What is the technology stack for implementation of the decentralized e-health privacy-conflict resolution system?

1.2.3 Roadmap & Structure

To answer this question, we develop an extended conflict-resolution ontology. What are the privacy conflict-resolution techniques when mapping the e-healthcare process to a blockchain? The definition of the privacy conflict-resolution technique aims to design a mapping between the e-healthcare process presented with BPMN into a blockchain-based system and specifies a proof-of-concept prototype. The remainder of the thesis is structured as follows. Chapter 1 introduces a running case and background preliminaries. Chapter 2 discusses the requirements for patient-centered PHR collection and processing. Next, the chapter addresses decentralized privacy conflict-resolution techniques and a selection of techniques for current research. Chapter 4 addresses the mapping the of designed BPMN e-Healthcare Process to a Blockchain System. Chapter 5 focuses on the implementation of a prototype for privacy conflict-resolution techniques. Chapter 6 presents an evaluation of a proof-of-concept prototype and compares the results of this research with other research work finally, Chapter 7 concludes the thesis together with providing indications for limitations, open issues, and future work.

1.3 Limitations

As healthcare ecosystem consists of numerous medical processes including hospital admissions, surgeries, discharge and billing, insurance claim, and many more. In this research, we have identified different important processes involved in e-healthcare that can lead to potential privacy conflicts, however, for the master's thesis research we have limited the scope to only 3 processes.

As blockchain provides more data security and transparency by exchanging encrypted data between peer-to-peer (P2P) networks. Because decentralized nature of blockchain creates a new concept of a token economy where the community's income can be shared between real content producers and service users who create value. A token is an object or symbol that is exchanged for goods or services, it is an immutable digital file or presentation of a contract. In the context of blockchain, tokens are built on top of the technology stack and represent value, and are predicted to lead to the emergence of the so-called token economy. In this current research, we do not focus on token economy, so the aspects of token economy and transaction cost will not be covered.

As maintaining privacy in user data is very important and failure to do this leads to implications related to legal sectors which are not covered in this research, so acceptance of proposed techniques depends on the country's legal law and hospital legal compliance.

Due to the scope limitation of the master's thesis, an initial prototype will be prepared, however, this prototype will not the fully ready for production.

1.4 State of the Art

A personal health record (PHR) system is an electronic record of a patient's health information. In PHR, patients can have full control and access to their medical information, they can trace all their medical history and contribute to their wellbeing [27] [28]. As PHR system can be managed by the patients, which enables them to share their personal information with related medical bodies and clinics in a cross-organizational structure. The PHR must include all relevant information about the patient's life, including a list of all problems, procedures that have been performed or scheduled for the patient, patient's underlying medical conditions, all allergies data, patient's monitoring data i.e., from home or through IoT devices, family, social and lifestyle history, list of all vaccinations, previous and current medications, list of laboratory tests with results, and patient's genetic data [29] [30] [31].

Electronic health records (EHR) are also called electronic medical records (EMR) and their use is becoming more and more popular in the context of e-health [32]. Electronic health records contain patients' health data and are confidential as a major factor in the application of e-health. An electronic health record consists of legal records that are compiled in a hospital setting. This data is then used as the main data source for the electronic health record [32]. PHR can take many forms: an independent stand-alone software application running on a single computer; a web service owned by one organization; a common web service as a platform for collecting various types of medical information; or USB based Plug and play PHR [33] [34].

Patient engagement [34] and Personal Health Record (PHR) systems solve the financing issues in healthcare as PHR supports patient-centered healthcare by availing medical records for patients and thus, assisting patients in health self-management [35]. The main purpose of PHR is that a patient is the author and owner of his/ her medical data that can be shared with other individuals, including healthcare professionals, or automated clinical decision-support services [36]. Research [35] defines values of PHR as communication improvement between a patient and a doctor, yielding patient education that results in lifestyle changes. Patient engagement simplifies personal health and well-being data collecting and processing that increases the value of personalized preventive healthcare services. Citation [37] predicts the emergence of a new category of personalized preventive health coaches who use the skills and the ability to interpret and understand health and well-being data. In the paper [38], authors define the economic and financial problems of the healthcare system and investigate the usage of blockchain technology to support decentralized and patient-centered systems. In a patient-centered system, a person creates and

manages his data while healthcare providers instead of owning it, use this data in their processes. The problem of transparent data sharing is described in [39]. Collecting and processing PHR creates various challenges related to legal, technical, and emotional issues. Researchers [40] [41] [42] focus on technical and security PHR-data requirements in the context of centralized PHR systems. This approach is efficient when the number of PHR data sources is limited. Thus, the number of processes that use PHR increases, and therefore, a centralized approach is not scalable. An integrated PHR and EHR system is socio-technical in that people as members of organizations try to collaborate and solve problems with the help of a very heterogeneous set of technologies [43]. The decision to use a patient-centric system that shares PHR is emotionally driven and creates feelings of insecurity in the way personal information is used. The usage of PHR integrated into EHR results in security, privacy, and privity conflicts. Privity is a legal term and restricts knowledge and control over the content and performance of a (smart) contract that should be distributed among parties only as much as is necessary [44]. A major issue with both PHRs and EHRs is the maintenance of electronic health records [32] because, for example, administrative staff can access information without the explicit consent of the patient [42]. The authors in [45] define data integrity, usability, auditing, and patient-information privacy as the main requirements that should be considered when developing medical systems in the Internet of Things (IoT) domain. Citation [46] points to cybersecurity and privacy issues during socially integrated mobile healthcare applications and provides a secured architecture for multi-cloud environments. The authors of [47] confirm that many users are concerned they do not have control over the collected medical data and are not aware of how it is used. Research [42] shows that for wearable devices, users do not understand security and privacy risks related to their data. The authors in [48] [49] [50] focus on the importance of security and privacy risks when sharing medical data and confirm that future work is required to provide the solution for building secure, integrated healthcare systems. Moreover, there are autonomous smart devices that are connected to smart home systems [35] and collect data related to the patient's health [46] [51] and measure specific medical data. To reduce the negative impact of conflicts in cross-organizational processes they can be either prevented or solved automatically if possible. Research [52] proposes the usage of equative algorithms for solving civil conflicts. These algorithms are based on different technologies such as artificial intelligence (AI) and algorithmic decision-making system (ADS). In [53] authors propose the usage of the Graph Model for Conflict Resolution (GMCR) for systematically investigating actual conflict occurring in the real world. Other researchers [54] use Hidden Markov Models (HMMs) to analyze the incoming data and handle the occurring conflicts. AnaThe analysiscludes adapting and training the Hidden Markov Models thatares later used in combination with a rule-based system to detect conflicting information, resolve the conflicts detected and use past data and decisions to avoid conflicts before they happen. Some researchers [55] propose the use of mediator that detects conflicts, suggest a possible solution to the conflicting parties. The systematic literature reviews [56] [57] [5] indicate that blockchain-technology research in healthcare is increasing each year in data sharing, health records and access control. A blockchain is a distributed ledger that allows participants to write and update records on a ledger and

cryptography ensures that records stored remain the same once added [58]. Records are added to the ledger in the form of transactions that are hashed and grouped in blocks where each block is cryptographically linked to the next block. A Merkle tree or hash tree is a cryptographical method that ensures transactions stored in a blockchain are linked with mathematical hashes [37] [38] to guarantee no modification can invalidate the entire record. The hashes provide an efficient method to verify any transaction on a blockchain and records can be verified without processing all stored data [37]. Computer programs that digitally verify, enforce contracts, and run on a blockchain network are referred to as smart contracts that are stored and executed on blockchain nodes. With the right access, any user can run and execute smart-contract functions from any participating node in a network [38]. Researchers [41] [59] propose the usage of ontologies to solve heterogeneous data-integration issues. An ontology is a formal description of the concepts and relationships that exist for an agent, or a community of agents. Research [60] addresses the gap in conflict modelling, management and resolution in business collaboration and propose a conflict-resolution ontology that is incomplete for the e-healthcare domain. We consider the combination of blockchain technology and ontologies as a means for solving security conflicts in integrated e-healthcare. Mostly researchers focus on the PHR processing and do not consider the integrated PHR and EHR in the cross-organizational processes. Research [60] focuses on conflict-resolution technology for cross-organizational processes while lacing a conflict-resolution ontology. This thesis research fills the gap in the privacy-conflict resolution for integrating PHR and EHR and extends the research [60] with a conflict resolution ontology for e-healthcare.

It appears from the literature that electronic health records make it easy to share structural health data between authorized health care providers to improve the overall quality of health care provided to patients. The use of e-health allows users to have a broader mindset and allows health care providers to work effectively online. Electronic health records make it very easy to share health information between stakeholders, as well as access and update patient information as the patient progresses through treatment. However, in such systems, security and confidentiality issues are very important, since the patient can face serious problems if confidential information is disclosed to a third party. From the reviewed articles for literature review and based on the analyzed areas of security, it becomes apparent that electronic health records use different rules and standards regarding privacy and security. However, it is necessary to uniform such systems to eliminate possible conflicts and inconsistencies between standards.

The Background Preliminaries to provide privacy conflict-management elaboration, we describe in Section 1.5 provides preliminaries required for understanding the next sections.

1.5 Preliminaries

2 Running Case and Privacy Conflict Scenario

The Running Case to provide privacy conflict-management elaboration, we describe in this section, a running case from the patient-centric perspective that simplifies the understanding of the running case and the remainder of this thesis.
In our running case, we assume that there are three partners of the insurance provider: the patient, a general practitioner from a hospital, and a healthcare professional which is illustrated in Figure 3. We consider there are different business rules for each stakeholder describing who is the claimer, and who gets paid by an insurance provider when specific conditions are met. In our running case, we consider that the systolic blood pressure measurement is used to determine the claimer. For the patient, a business rule states, "If the patient's systolic blood pressure is less than 160, the patient is the claimer; else the claimer is a general practitioner". In common practice, a systolic blood pressure of 120 is defined as a normal value and thus, the patient does not have any problems related to the blood pressure now. The decision assumes, that if the patient does not have any problems, his lifestyle is good, and he is a claimer for the insurance provider. The systolic blood pressure between 120 and 160 is considered problematic and requires patient attention and activity to bring it back to normal. Thus, the patient considers himself a claimer in this data slot as well. Systolic blood pressure that is higher than 160 is considered dangerous and requires a doctor’s attention. Therefore, the patient considers the general practitioner as a claimer.

For the general practitioner, a business rule states that "If the patient's systolic blood pressure is less than 120 then the patient is a claimer and otherwise the claimer is a general practitioner". In case the patient's systolic blood pressure is out of the norm, that is 120, the general practitioner monitors the patient and prescribes required medications and procedures based on the initial testing. Therefore, the general practitioner considers himself a claimer.

Finally, the healthcare professional has his own business rules stating "If the patient's systolic blood pressure is less than 120 then the claimer is a patient; if systolic blood pressure is higher than 160 then the healthcare professional is a claimer; otherwise, if systolic blood pressure is between 120 and 160, the healthcare professional does not specify the claimer".

The internal rules of all three stakeholders create conflicts that are illustrated in later section 4. The conflicts occur when a patient's systolic blood pressure is higher than 120.

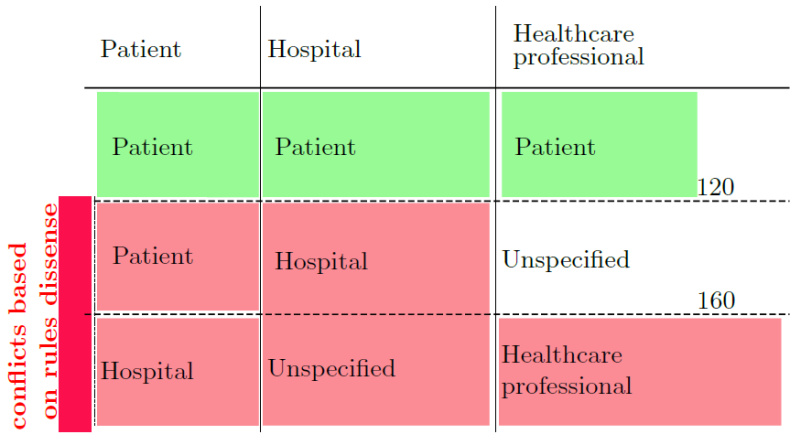

Figure 3. Business rules caused behavior conflicts.

Figure 4 describes the running case in the cancer-prevention domain to understand the conflict scenario. While the most used clinical outcome measures by physiotherapists are pain, range of motion, and strength, the patient-goal domains are identified as physical activity, quality of a workplace, and sleep. Such a difference is explained by the fact that The Patient-Specific Functional Scale [90] comparison between individuals is difficult and thus, patient goal domains cannot be measured. Suppose a patient monitors himself at home with different autonomous devices such as a smart watch and components of a smart home such as air and water quality sensors, these devices collect data about a patient's activities and ecological environment. The devices communicate with each other sharing the data if needed. This data is being collected continuously enabling the feedback loop for a healthcare professional who monitors the patient. In parallel, during the patient's visit to a doctor, the latter creates EHR data that include laboratory test results and anamnesis. Both healthcare professionals and a doctor have access to EHR. After treatment is performed, a healthcare specialist and general practitioner send their medical reports to the insurance provider requesting claims. The medical reports differ because the data available for the healthcare professional includes PHR and continuous feedback from the patient. This improves the health context understanding and results in personalized care provided by the healthcare professional. For the doctor, only EHR is available and thus, his focus is on employing conventional Western school medicine for treatment that relies a lot on administering medication. Both, general practitioners, and healthcare professionals share collected medical data to request compensation from the insurance provider. The difference in claiming medical data leads to the conflict with the insurance provider who does not have guidelines for PHR data processing. Such a gap complicates the usage of new medical services based on the PHR processing and a feedback loop has the potential to improve the current healthcare system.

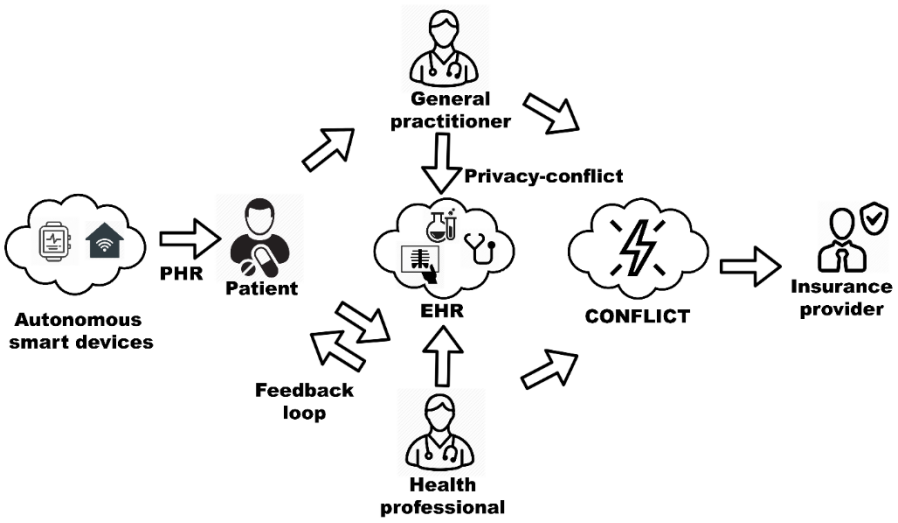

Figure 4. Conflicts in the EHR and PHR processing.

The patient faces privacy conflicts as his data can be stolen due to a lack of security in either smart autonomous devices, or different applications. After the patient shares his PHR with the family doctor, the latter can use it in the internal processes of the healthcare provider, e.g., for reporting, statistics, and research. These processes may include external stakeholders such as the national statistics department, private research companies, or private companies specializing in reporting services. As such, processes are not transparent to the patient and thus, inappropriate use of PHR data may occur.

In our research, we define five conflicts when integrating PHR and EHR. First, privacy conflicts occur when the patient collects data during home monitoring. The use of wearable devices and PHR systems that store collected data can be vulnerable to stealing data by unauthorized persons. A privacy conflict occurs after PHR is shared with a family doctor, integrated with EHR, and then shared by the doctor with external stakeholders. The internal processes of healthcare providers are not transparent to the patient and thus, result in inappropriate use of the patient's information. Third, integrity conflicts occur when PHR flows through different processes and can be modified by the stakeholders. Then, a consistency conflict exists when the family doctor accepts or rejects shared PHR before the integration with EHR. A data-consistency conflict occurs when the family doctor decides to accept or reject shared PHR before integrating it with EHR. A doctor can wrongfully reject the correct data due to perceived unreliability, or the uselessness of the healthcare plan. The decision of a doctor is based on the respective healthcare provider- and national regulations and results in conflicting medical- and administrative rules. Finally, the consistency conflict occurs when the insurance provider receives claims from both the healthcare professional and the doctor who provides different data in the insurance claim.

3 Identification of privacy conflicts in the e-health cross-organizational processes

Improving the delivery of care is one of the main driving factors of the transformation strategy aimed at improving the quality of care while reducing costs. Medical processes include hospital admissions, discharge and billing, emergency department (ED), Surgeries, patient transfers, medications, patient flow, and many more. Thus, healthcare processes affect operations, patient experience, and physician job satisfaction throughout the healthcare system. In this chapter, first section 3.1 is the identification of important processes in e-health cross-organization. Next, section 3.2 focuses on requirements for the Patient-centric PHR Collection and Processing. Finally, section 3.3 describes privacy conflicts in e-health cross-organizational processes.

3.1 Important processes of e-healthcare cross-organizational process

Healthcare management involves many processes such as managing finances, staff, patients, legal issues, logistics, inventory, etc. In the following section, we have identified important processes of e-healthcare in the cross-organizational process which can lead to the identification of privacy conflicts.

3.1.1 Patient Internal Process

The internal patient data collection and claimer definition process are shown in Figure 4. When the insurance provider prepares a claim, he asks the patient to provide the blood pressure measurement. We assume that patient uses some application where his data is stored. First, the patient checks if the required data exists in his PHR and, if not, measures his blood pressure and saves it in the system. Next, the patient retrieves the data from the system and, if data can be shared with others, shares it with the insurance provider. For the simple reason, we do not consider the processing of PHR that cannot be shared, also, the data privacy policy can be different from system to system and is out of the current research scope.

3.1.2 Healthcare Provider Internal Process

The internal general practitioner data collection and claimer definition is an important process that involves different cross-organizational stakeholders. The insurance provider prepares a claim, he asks the general practitioner to provide the blood pressure measurement. The patient can record his information using different IoT wearables which will lead to a non-standard format of data causing data mismatch conflict.

3.1.3 Healthcare Professional Internal Process

The internal healthcare professional data collection and claiming process is one of the important e-healthcare processes as it involves multiple entities from cross-organization. In this process, the patient provides his medical personal data and allows access to a healthcare professional. When

the insurance provider prepares a claim, he asks the healthcare professional to provide the blood pressure measurement. The healthcare professional has access to both PHR and EHR and shares the information with the insurance provider.

3.1.4 Procedure for e-prescriptions for medicinal products

In e-health systems, one important workflow is prescription, which aids to improve patient safety, better monitoring services, and quality of healthcare. Prescriptions are part of a patient's treatment and medical record history; it needs to be shared across different stakeholders within and across organizations. The doctor writes prescriptions for the patient. Doctors and patients give access to the e-prescription to pharmacies to prepare and send the correct and required dosage of prescribed medicines to the patient.

3.1.5 Sharing Laboratory Test/Results Data

Suppose a patient monitors himself at home with different autonomous devices such as a smart watch and components of a smart home such as air and water quality sensors, these devices collect data about a patient's activities and ecological environment. The devices communicate with each other sharing the data if needed. This data is being collected continuously enabling the feedback loop for a healthcare professional who monitors the patient. In parallel, during the patient's visit to a doctor, the latter creates EHR data that include laboratory test results and anamnesis.

3.2 Requirements for the Patient-centric PHR Collection and Processing

To define the requirements for the patient-centric PHR collection and processing, we provide in Section 3.2.1 a value proposition for the designed system, its sub-goals, and actors. The defined goals and actors are used to create a role and organizational model in Section 3.2.2 that describes the responsibilities and constraints of individual roles in the system.

3.2.1 Goal Model of the Personal-Centric System

According to [83], analyzing the problem of this socio-technical domain can be performed by using a goal model. The objective of goal models is to serve as a communication medium between technical and non-technical stakeholders for generating understandable domain knowledge. To achieve the goals, the derived system needs capacities or functions that are described as roles. We use role models to present the relations between different roles defined in the derived system. Figure 4 presents a goal model, comprising functional, quality, and both positive and negative emotional goals with each functional goal decomposed into sub-goals hierarchically from top to bottom. In the previous research [48], the authors used goal models in the context of requirement engineering. We use the notation described in [82] where the heart, cloud, and parallelogram shapes represent the emotional, quality, and functional goals respectively.

The value proposition is prevented disease related to an individual who feels self-motivated and expects to be informed and empowered during the whole preventive process. The system provides

advantages to the individual to prevent disease in the future. The sub-goals: provide home care in a trustable manner, provide ambulatory care, provide insurance performed by an insurance provider, and onboard stakeholder performed by an acceptor agent.

The onboard stakeholder goal is required for the stakeholders to participate in the cross-organizational process. Both, a healthcare specialist, and a general practitioner submit medical cases to the insurance provider for requesting claims. The first comprises two further sub-goals, namely monitoring health status performed by the smart-hub agent and keeping a healthy lifestyle that involves the role of a health professional.

The latter uses the system if feels that he is confident in the system, can take professional decisions, and is not overloaded with the system complexity. Finally, both patients and health professionals can propose insurance claimers based on their internal decision rules.

The monitor health status goal has three sub-goals: create PHR based on the collected data of two agents: smart watch and air quality home sensor, analyze PHR with the minimal participation of an individual, and share PHR that processes the interoperable and up-to-date information securely. Created PHR is integrable so that it can be shared with other stakeholders. Individuals worry about data misuse when sharing PHR. To keep a healthy lifestyle goal includes two sub-goals: provide health guidelines and assess current lifestyle. Guidelines should be personalized and usable for the patient.

The goal provides ambulatory care involves the role of a general practitioner who is afraid to be replaced by the tool and requires feeling professional and not overloaded. The goal has three sub-goals: create EHR that is integrable, accept shared PHR, and conduct a medical diagnosis. When accepting PHR, a general practitioner has concerns about shared data accuracy. Medical data often is stored in different standards and has different contexts led to semantic heterogeneity. Standardization of the PHR and EHR data helps to avoid that. Also, such a standardization simplifies PHR- and EHR processing. The acceptance of PHR should be secure, integrable, and usable. A general practitioner can also propose an insurance claimer based on the internal decision rules.

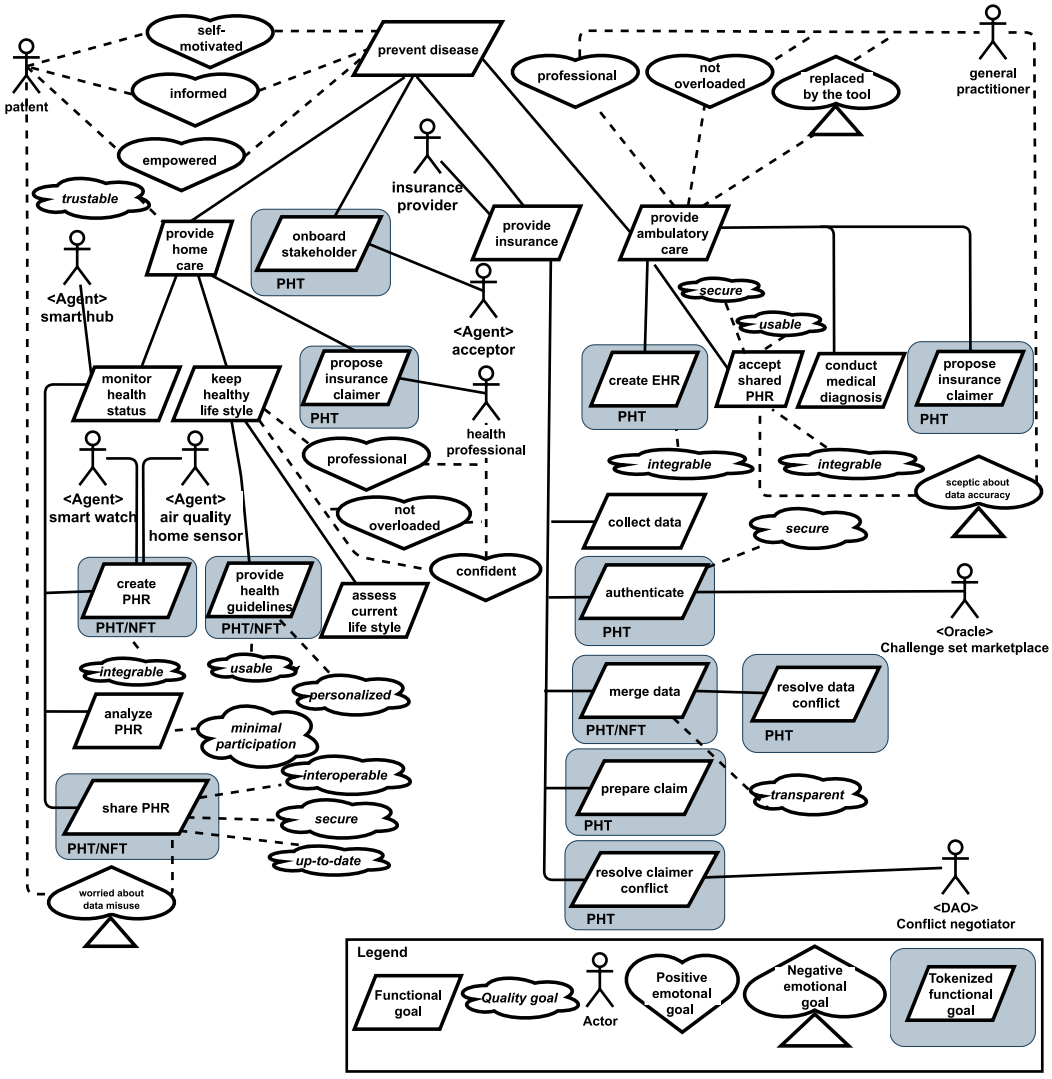

Figure 5. The goal model for the personal-centric system.

The provide insurance goal has five sub-goals: collect data, authenticate, merge data, prepare a claim, and resolve claimer conflict. The collected data is used during the claim preparation and requires authentication for data sources in the cross-organization process. To prepare a claim the insurance provider is required to merge data transparently and merge data conflict if present. As every stakeholder has its own business rules defining the claimer, the insurance provider needs to resolve claimer conflict if such occurs.

3.2.2 Role and Organization Model

The goal model defines the value proposition of the derived system. Role models represent the responsibilities and constraints of individual roles required by the system. In socio-technical systems, both human- and manmade agents have responsibilities. In [52], the authors notice that positions in organizations are described in terms of responsibilities and constraints.

Figure 5 depicts an organizational model for a system consisting of humans and autonomous smart devices that communicate with each other without human intervention [77]. This organizational model includes control and peer relationships. A patient creates PHR from data collected by autonomous smart agents, i.e., a smart watch and an air-quality home sensor that communicate with each other as peers. To simplify the creation of PHR that is collected by different smart devices, we propose a smart-hub component that represents the interface for the patient and the doctor who does not need to communicate with each device directly. A smart hub controls the autonomous smart devices and provides the patient with the data used when creating PHR. The patient shares PHR with the healthcare professional while being treated by the general practitioner.

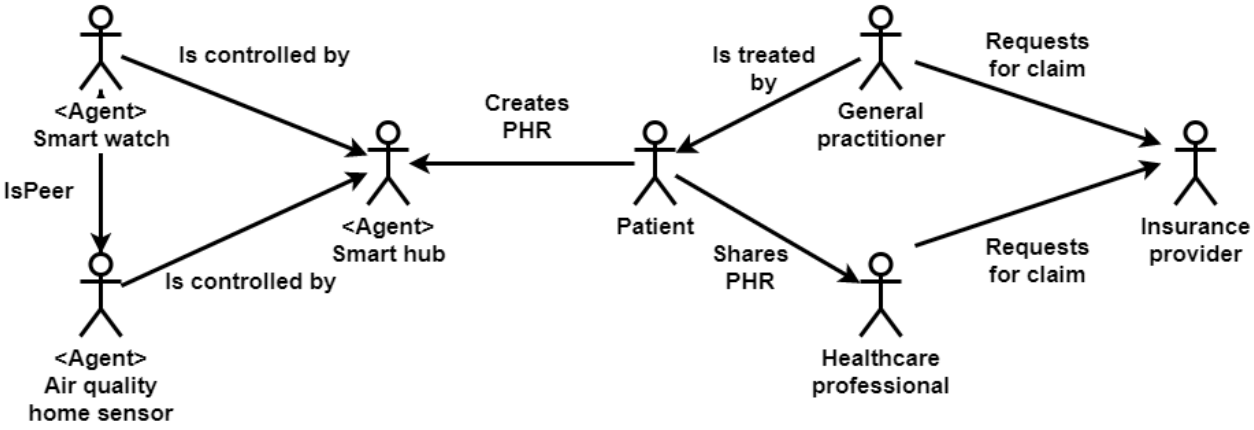

Figure 6. Organizational model of PHR creation and sharing processes.

3.3 Privacy conflicts in e-health cross-organizational processes

In e-healthcare cross-organizational processes, multiple stakeholders are involved and collaborate. Cross-organizational communication can be a potential point of conflict. Below mentioned figure 7 gives a better understanding of conflict lifecycle and the explains the approach used in research [60] for conflict identification and classification:

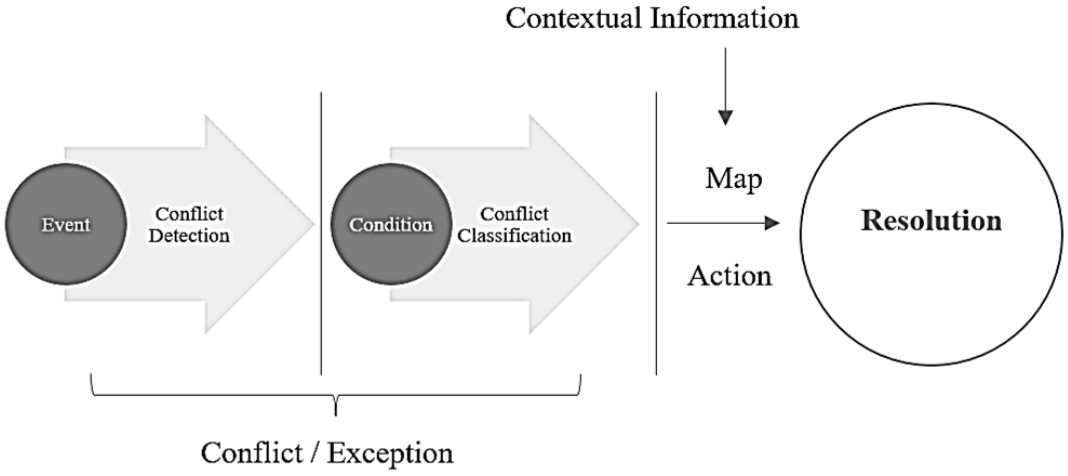

Figure 7. Conflict Resolution Lifecycle

The first step in the process of conflict resolution lifecycle is to identify the conflict type, origin, and its impact on the rest of the components. Once the conflicts are identified next phase is to implement a conflict resolution strategy. In this research, we defined five conflicts using the techniques identified in research [60] when integrating PHR and EHR which are mentioned in the given below sub-section.

3.3.1 Data Collection Conflict

First, a privacy conflict occurs when the patient collects data during home monitoring. The use of wearable devices and PHR systems that store collected data can be vulnerable to stealing the data by unauthorized persons.

3.3.2 Transparency of Internal Processes to External Stakeholders

A privacy conflict occurs after PHR is shared with a family doctor, integrated with EHR, and then shared by the doctor with external stakeholders. The internal processes of healthcare providers are not transparent to the patient and thus, result in inappropriate use of the patient's information.

3.3.3 Integrity Conflict Across Different Processes

An integrity conflict occurs when PHR flows through different processes and can be modified by the different stakeholders in a cross-organizational structure. Then, a consistency conflict exists when the family doctor accepts or rejects shared PHR before the integration with EHR.

3.3.4 Data Consistency Conflict

A data-consistency conflict occurs when the family doctor decides to accept or reject shared PHR before integrating it with EHR. A doctor can wrongfully reject the correct data due to perceived unreliability, or the uselessness of the healthcare plan. The decision of a doctor is based on the respective healthcare provider and national regulations and results in conflicting medical and administrative rules. Finally, the consistency conflict occurs when the insurance provider receives claims from both the healthcare professional and the doctor who provide different data in the insurance claim.

3.4 Conclusion

Chapter 3 focused on the first research question of how to identify privacy conflicts in the e-health cross-organizational processes. In first section 3.1, to answer the first sub-research question we defined disease prevention as the main process which can have possible privacy conflicts because of data exchange and communication among different systems i.e patient-, healthcare provider-, healthcare professional, and insurance. Next section 3.2 identifies the requirements for conflict identification with the goal model and these requirements include insurance provision and transparently merging healthcare data. Finally, in section 3.3 we have defined data collection

conflict, transparency of internal processes to external stakeholders, integrity conflict across different processes, and data consistency conflict.

The first section of the chapter corresponds to the first sub-research question (SRQ-1) where we identify important processes for cross-organizational e-health that can be used as pilot ones for adopting blockchain technology. Such processes are person-centric and focus on disease prevention, a better quality of life, and healthcare insurance involving different stakeholders from the healthcare ecosystem i.e doctors, patients, healthcare professionals, and insurance providers.

Next, we provide a more detailed set of requirements for outlined processes that address the second sub-question SRQ-2. Since the AOM goal model lacks emotional-, and blockchain context, we extended our goal model with emotional-, and tokenized goals. Requirement definition highlights patients' concerns while sharing personal data and lack of trust towards medical data created by other stakeholders.

Finally, the last section answers the third sub-research question (SRQ-3), where we identify privacy conflicts i.e data collection, transparency, integrity, and consistency that exist during healthcare data integration and sharing. To identify resolution techniques, the definition of privacy is required as an initial step. As we used the conflict resolution strategy from research [60] because the literature review showed that it is a relevant approach for categorizing the conflicts and impact analysis which results in the selection of top priority conflicts.

To conclude this chapter, it can be said that the extension of the goal model that has been done in this research is helpful to identify privacy-oriented processes. Thus, this approach can be useful for the development of blockchain-based e-health systems on a larger scale. Developing healthcare services requires privacy conflict resolution techniques. While identifying privacy conflicts usage of conflict resolution strategy previously used in Service-oriented cloud computing for virtual enterprises proves to be relevant in healthcare cross-organizational processes as well.

In this research, we only have selected important processes due to limit and scope constraints, however, for future work multiple processes can be selected and conflicts related to them should be identified for resolution. Process selection can be done by interviewing or taking a hospital onboard to have real-life processes and existing conflicts.

4 Privacy Conflicts Resolution in PHR & PHR between Patients and Healthcare Providers

Modern information technologies are increasingly being used in healthcare to the quality of medical services and reduce costs. Internet of Things is one of the leading technology and hot topics for researchers, and technology specialists. Internet of Things (IoT) has revolutionized the healthcare sector by providing IoT-based healthcare wearables which improve patients' lifestyles and help in preventive disease management. As patient uses different devices to record his medical data, which leads to different conflicts as identified in section 2.3. In this chapter, privacy conflict resolution techniques will be identified which can help to resolve the identified conflicts. In Section 4.1, the literature review is performed to study existing decentralized techniques for privacy conflict resolution. Next, section 4.2 describes the approach used in this research to map privacy-conflict techniques to a decentralized healthcare ecosystem.

4.1 Existing Decentralized privacy conflict-resolution techniques

To explore what existing techniques are being used to resolve the conflicts we performed the literature review and found very limited research using blockchain-based privacy conflict resolution for the healthcare domain. Research [67] proposes an architecture for a smart e-health gateway that not only reads but also processes the gathered medical data. Research [60] follows the conflict-management lifecycle mentioned in the previous section's figure 7 and provides a conflict resolution technique for virtual enterprises. Research [60] defined conflict strategies as the combination of conflict type and collaboration sub-patterns. Conflict resolution starts with setting up business rules which cause conflict. During conflict resolution, it is determined which business rules will be removed or overwritten to resolve the conflict.

Research [91] considered Decentralized Autonomous Organizations (DAOs) for decision making, which are based on the concept of running both commercial and non-commercial enterprises without following a traditional management structure. Execution of inter-organizational business process is executed by blockchain smart contracts that result in decentralized autonomous organizations (DAOs) [91]. DAO's rules and regulations are also stored on the blockchain to keep rules transparent to the stakeholders. As DAOs provide significant results in terms of decision making and performance is the reason to select the usage in current research to resolve the privacy conflict and extended to the healthcare business processes in a cross-organizational context.

4.2 Criteria for the decentralized privacy-conflicts resolution techniques

In this research, we map the privacy-conflict resolution approach technique presented in [60] into a decentralized healthcare ecosystem that includes autonomous smart devices and collaboration between them as described in [68]. To resolve privacy conflicts during the integrated health-data

processing, we extend the conflict ontology defined in [91] using the Prot´eg´e tool[11] together with the Web Ontology Language (OWL)[12] [81]. The ontology that describes contract-based business processes and include conflicts together with their reasons (internal business rules) and possible consequences (remedies).

The processing of integrated EHR and PHR in the cross-organizational processes requires an ontology definition to simplify the definition of contracts used between stakeholders in the cross-organizational process and to simplify the PHR and EHR data heterogeneity. As the conflict-resolution techniques are based on the contract's legal aspects and data involved, the ontology is also useful for defining such techniques as smart-contract blockchain technology.

To present conflict-resolution techniques, we provide the integrated e-health ontology that extends the previous research [91] and includes the ideas about legal contracts. In this research [91], they proposed to consider DAOs as Virtual Enterprises (VEs), where each enterprise is a collaborating part of a peer-to-peer network and is governed by smart contracts that constrain the behavior of each enterprise. Each enterprise is a decentralized, self-organized network, and works autonomously on the blockchain. In the context of DAOs, enterprises are the peers or agents which provide specific functions for collaboration. DAOs are defined with Smart Contracts and use peer-to-peer serverless computing providing a loosely coupled collaboration. Research [91] also represents the verified common smart-contract languages (SCL) ontology to specify different types of legally binding collaborative smart contracts. The ontology is developed with the Protégé tool[13] for systematic knowledge acquisition [87]. We present the most relevant ontology concepts such as smart contracts, rights and obligations, and healthcare information with separate diagrams.

[11] https://protege.stanford.edu/
[12] https://www.w3.org/2001/sw/wiki/OWL
[13] https://protege.stanford.edu/

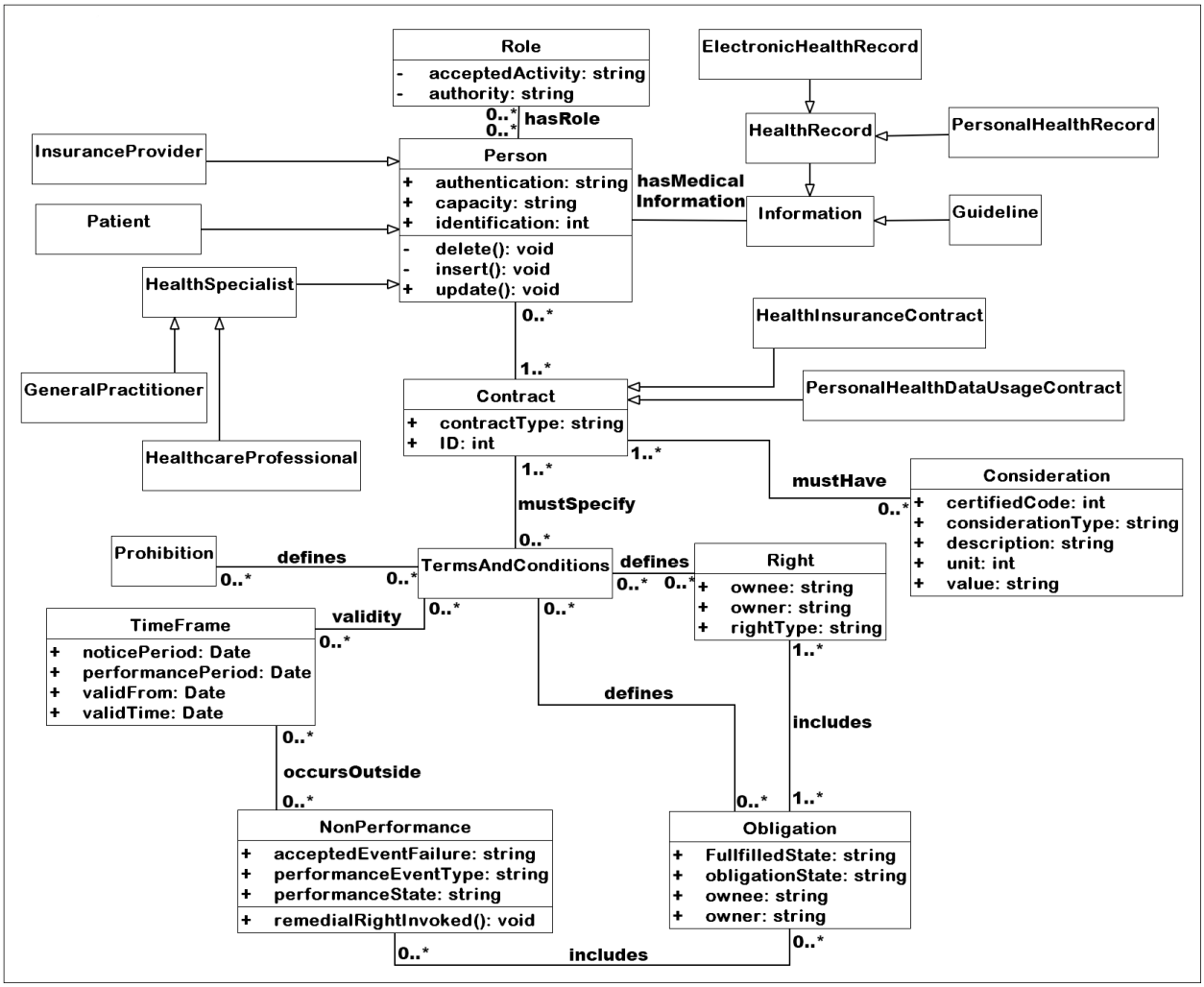

Figure 8. Upper level for the smart-contract ontology in e-health.

Figure 8 defines the upper level for the smart-contract ontology and based on the ontology defined in [42], the contract is an agreement between one, or more contracting parties that are represented in our running case as a patient, general practitioner, healthcare professional, and insurance provider. Both general practitioners and healthcare professionals are health specialists. Each contracting party has a role that defines its accepted activities and authority. As the ontology of this research focuses on the healthcare domain, each contracting party has medical information including medical guidelines and PHR and EHR as health records. In our running case, the contract is limited to the health insurance- and personal health-data usage contracts and has terms and conditions that include obligations, rights, prohibitions, and time frames that need to be agreed upon by the contracting parties.

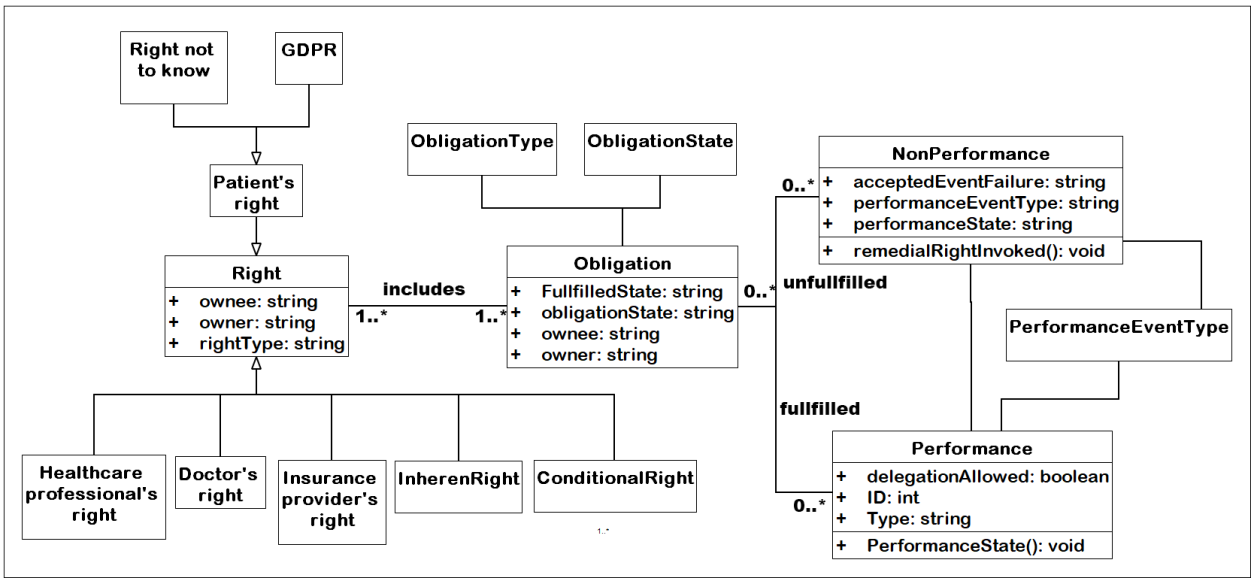

Figure 9. Healthcare obligations and rights.

Figure 9 focuses on obligations and rights for healthcare contracts. For example, the patient's rights include General Data Protection Regulation (GDPR)[14] and the Right Not to Know (RNTK) [44]. There are several obligations for a patient such as sharing personal information when having a positive COVID-19 diagnosis that can include location, list of contacts, etc. Additionally, a patient obligation may include mandatory vaccinations for visiting certain regions, e. g., visiting Africa requires the yellow-fever vaccination or having a COVID-19 vaccination when traveling to European countries. There are several possible conflicts available in our running case and several possible remedies for a patient. For example, if GDPR or RNTK rights are violated, a patient can ask for compensation and prepare a legal claim. On the other hand, if a patient violates obligations, this may result in a state-issued fine, when not sharing required information with a national health system when testing COVID-19 positive, or a lack of vaccinations arises for traveling to specific regions. At the same time, obligations and rights comprise conflicts on a fundamental level in healthcare, e.g., one of the basic humans right for free traveling is restricted due to the COVID-19 pandemic.[15]

The obligation of a general practitioner includes providing health services to everyone who needs them, sharing the patient health information - and providing reports to public health services. The general practitioner's rights enable the patient's information storage and -processing, selecting the treatment, and setting the diagnosis. If a conflict occurs related to the rights, or obligations of a general practitioner, there are several remedies available. First, a doctor can be fined or receives a financial claim from a patient, or legal institution if he refuses to provide required healthcare services. Legal institutions may also cancel the medical license for general practitioners in such cases. The healthcare professional has a right to store and process a patient's information and share

[14] https://www.gdpreu.org/
[15] https://covid19.who.int/

it with external providers if agreed by the patient. Additionally, the healthcare professional needs to provide a health plan to the patient. In case the health plan is not provided or results in damage to the patient's health, the patient may claim compensation and initiate a legal issue.

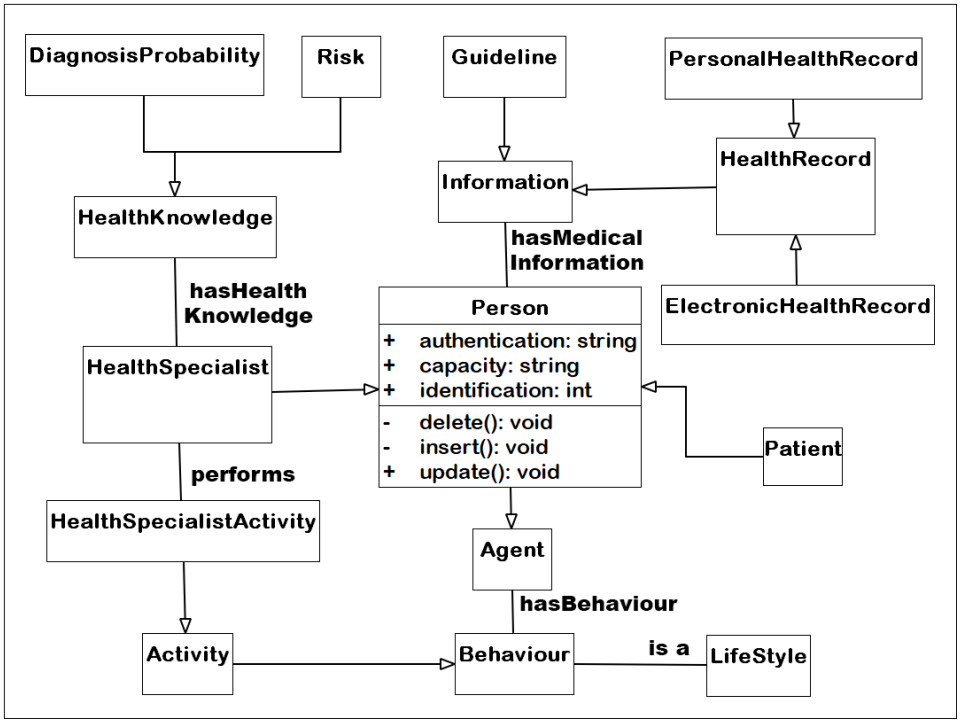

Figure 10. Healthcare-related information and activities.

Finally, the insurance provider has the right to ask for medical data from contracting parties and deny payments if the case violates the terms and conditions agreed. The insurance provider's right is to store and process medical data. The main obligation of the insurance provider is to perform payouts. There are several remedies for the insurance provider. First, he may refuse to process the claim payment if no agreed medical data is provided. If a contract's terms and conditions are violated, the contracting parties may file a court case.

Figure 10 describes the concepts specific to the healthcare domain that are involved in the running case's contracts. These include health information, behavior, and health knowledge. Health specialists, both general practitioners, and healthcare professionals' access medical information that includes guidelines and health records. To provide healthcare services, a specialist requires health knowledge that includes an understanding of risk- and diagnosis abilities as input for the creation of a personalized health plan and treatment processes. In the previous research [92], we define agents that can be both human and non-human. Agents are active participants of the decentralized system, and their actions are based on their behavior. In our running case, e.g., a patient has a lifestyle that includes healthy activities and dangerous habits such as smoking, alcohol consumption, and extreme sports activities.

Next, we use the proposed ontology for defining the privacy conflicts that arise between different agents in the cross-organizational processes. We consider healthcare processes as contract-based where all agents have their behavior, obligation, and rights assigned. The formal representation of the privacy conflicts and the decentralized nature of the cross-organizational healthcare processes result in developing the conflict-resolution techniques in the blockchain-based system.

4.3 Conclusion

In this chapter, we proposed privacy resolution techniques. In the first section 4.1, where a literature review is performed to find existing techniques that are used currently in decentralized e-healthcare systems to resolve privacy or data sharing conflicts. In the next section 4.2, we defined criteria for decentralized privacy resolution techniques with an ontology that describes contract-based business processes and includes conflicts together with their reasons (internal business rules) and possible consequences (remedies).

The first section of the chapter corresponds to the first sub-research question (SRQ-1) we performed a literature review of existing blockchain-based decentralized techniques in e-health systems which helps to resolve the privacy conflicts. Existing approaches include the usage of an architecture for a smart e-health gateway that not only reads but also processed the gathered medical data conflict-management lifecycle to provide a conflict resolution technique for virtual enterprises and defined conflict strategies which are a combination of conflict type and collaboration sub-patterns.

The second section addresses the second sub-research question (SRQ-2) where we provided the criteria for selecting the existing techniques from other technology domains for the healthcare domain as there were no blockchain-based techniques for cross-organizational context in the healthcare domain.

To conclude this chapter, a proposal to resolve the conflict using blockchain-based techniques instead of the traditional way would provide a decentralized and autonomous solution with a high degree of security and privacy. Currently, privacy-related conflicts are handled in a traditional way that is not time and money efficient. Healthcare cross-organizational domain acquires its ontology that must be customized according to healthcare needs. Cross-organizational processes we need to have autonomous conflict resolution techniques based on different stakeholders, and goals.

In the current research, we do not consider healthcare data in detail, and we did not use a healthcare specifier but rather used general data. Security threats and vulnerabilities related to the autonomous approach can be taken for future work as they were not included in the scope of current research.

5 Mapping the BPMN Designed e-Healthcare Processes to a Blockchain System

The development of blockchain applications is complicated due to the immutability of smart contracts and therefore requires proper design and testing in the early stage of development. Research [67] proposes an architecture for a smart e-health gateway that not only reads but also processes the gathered medical data. In this research, we map the privacy-conflict resolution approach technique presented in [60] into a decentralized healthcare ecosystem that includes autonomous smart devices and collaboration between them as described in [68].

We use a model-driven engineering (MDE) approach defined in research [59] to create well-tested smart-contract code. In [59], the approach starts by defining the business process with BPMN notation and then using the Lorikeet tool to translate the BPMN notation to the smart-contract code. We design the insurance-claimer-definition process with BPMN notation in Figure 8. The insurance-claimer-definition includes retrieving data from PHR and EHR data sources, their integration, and filtering out noise data. We split the cross-organizational process of the claimer definition into the three sub-processes: healthcare professional-, healthcare provider- and patient-internal decision-making process. Next, we present three internal processes with the BPMN notation. Figure 11 describes the internal decision-making process for the patient based on the business rules defined in Section 4. First, the patient checks if the requested data by the insurance company exists in his PHR repository. If the requested data is missing, the patient measures the blood pressure and saves new data in the PHR repository. Then, the patient retrieves it from the PHR repository for sharing with other stakeholders of the cross-organizational process. Finally, to propose the claimer, the value of the blood pressure is checked. If the blood pressure value is less, or equal to 160, the patient proposes himself as a claimer. Otherwise, the healthcare provider is proposed as a claimer. Figure 10 describes the internal decision-making process for the healthcare provider, e.g., a hospital. First, the healthcare provider retrieves the illness (EHR) data from external EHR systems that may be part of a hospital. After external EHR data is retrieved, this data is converted to the healthcare provider's health-data standard and saved in its system. After external data is imported to the healthcare provider's internal system, it is shared with the other stakeholders of the cross-organizational process.

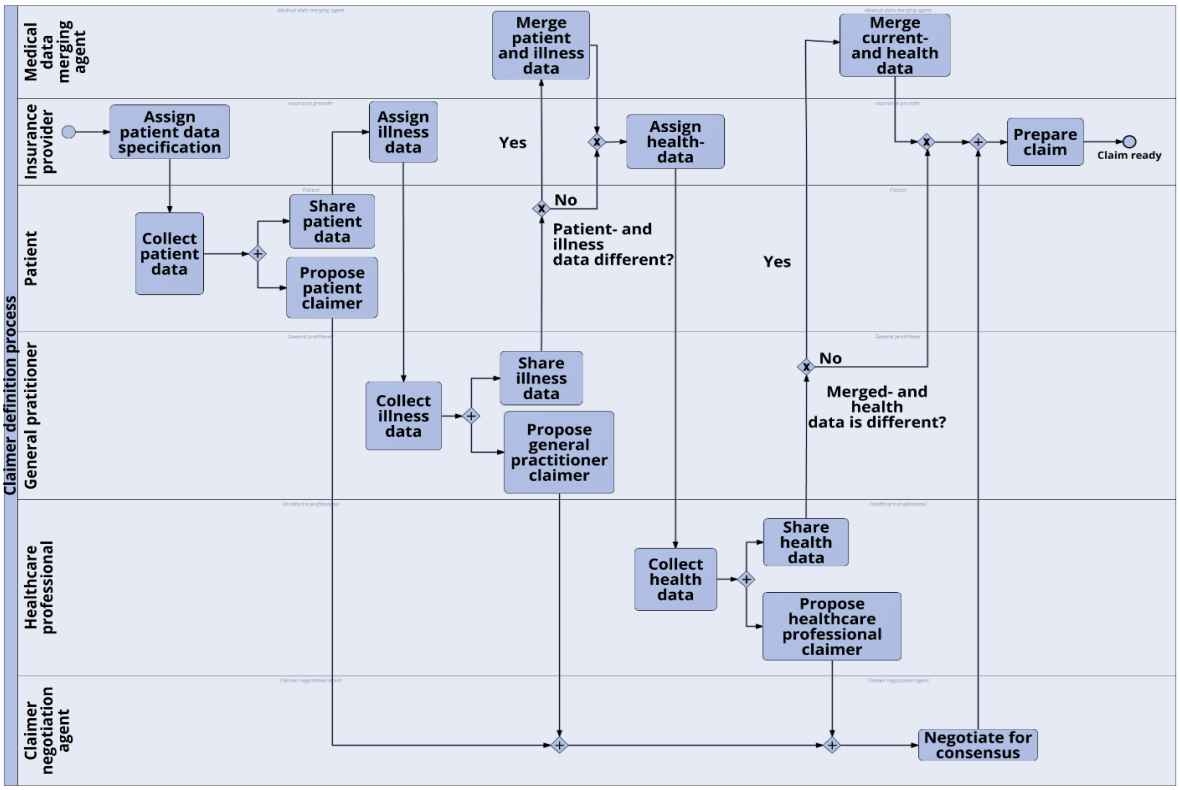

Figure 11. Claimer-definition process for the insurance provider.

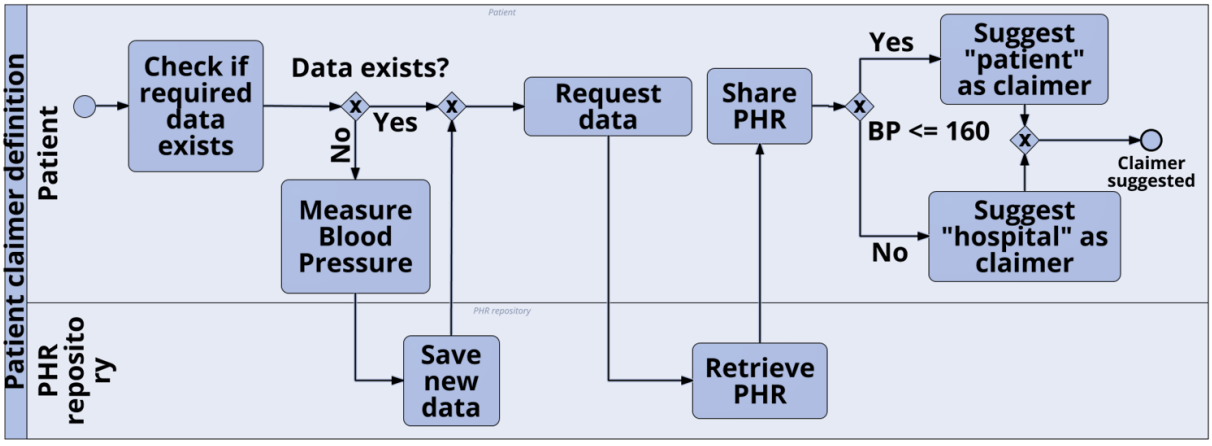

Figure 12. Patient-claimer internal decision process.

Finally, the healthcare provider's claimer proposal is based on the business rules defined in the previous section. There are three possible proposals: patient, healthcare provider, and undefined claimer. First, if the blood pressure value is less, or equal to 120, the patient is proposed as a claimer. If the blood pressure value is more, or equal to 160, then the claimer is not proposed. Finally, the healthcare provider is proposed as a claimer if the blood pressure value is between 120 and 160.

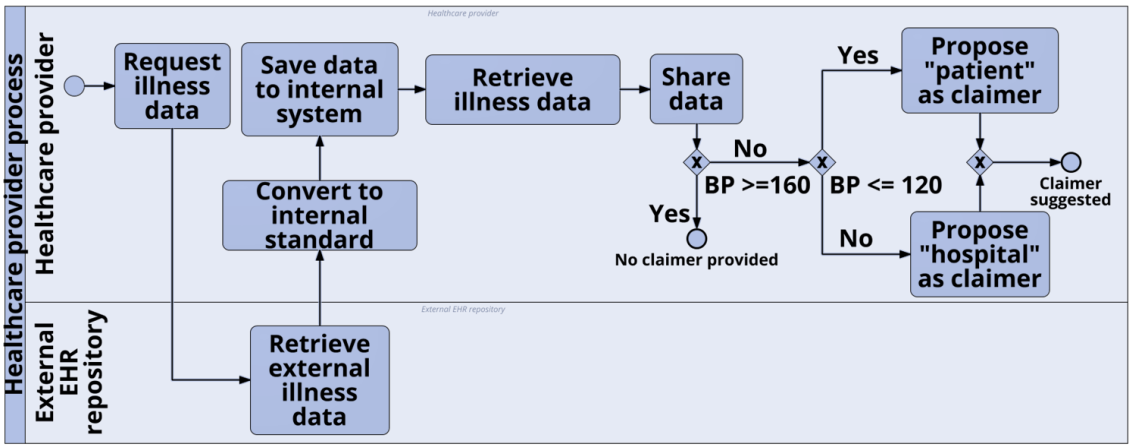

Figure 13. Healthcare-provider claimer internal decision process.

Figure 13 describes the internal decision-making process for the healthcare professional. The main difference between the patient- and healthcare provider. decision-making processes are that healthcare professionals have access to both EHR and PHR data.

First, blood-pressure measurements are retrieved from PHR and EHR repositories in parallel. After filtering out the noise data, the healthcare professional proposes the claimer. If the blood pressure is less, or equal to 120, the patient is offered a claimer. If the blood pressure is between 120 and 160, the claimer is not defined. Finally, if the blood pressure is more than, or equal to 160, the healthcare professional proposes himself as a claimer. The EHR and PHR integration part is based on the previous research [48] and business rules for the claimer proposal are defined in Figure 13.

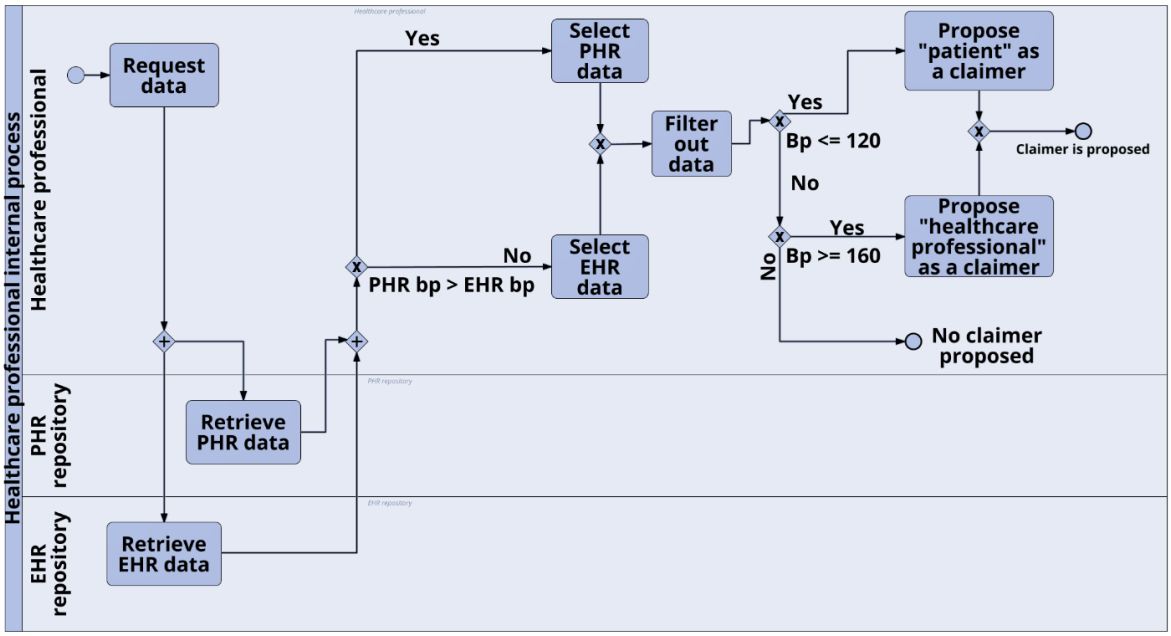

Figure 14. Healthcare professional claimer internal decision process.

5.1 Architecture

Before the implementation of the proof-of-concept prototype, we define the architecture of the system in Figure 15. There are different types of blockchain that support smart contracts. The proposed system can be split into three layers: orchestration, choreography, and DAOs. The orchestration layer communicates with stakeholders' systems such as patients, hospitals, healthcare providers, and insurance systems. Stakeholder's authentication can be established by designing Authcoin that offers M2X token economy, self-sovereign, configurable multi-challenge set identity authentications for humans and machines that are managed with means of smart contract blockchain technologies however, in the current prototype due to time constraints we focused only on the design and implementation can be taken as future work. In our context we propose the usage of Ethereum smart contracts for patient, hospital, and healthcare professional systems and Polygon[16] smart contracts for insurance provider systems. To enable interoperability between different blockchain-based systems we use Polkadot. Polkadot enables scalability by allowing specialized blockchains to communicate with each other in a secure, trust-free environment. Polkadot serves as a foundational layer of a decentralized web, where users control their data and are not limited by trust bounds within the network. For the DAO layer, we use Ethereum smart contracts that provide simple voting mechanisms. The DAO voting algorithms are out of scope in the current research.

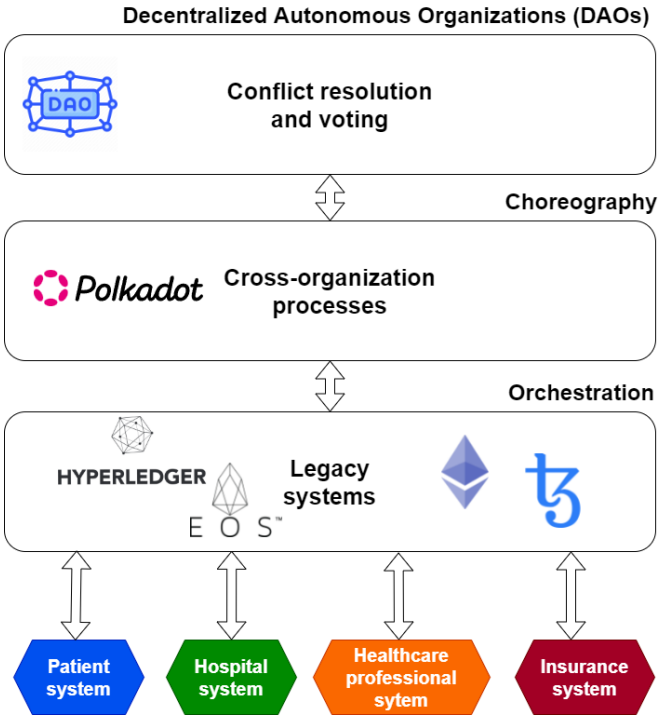

Figure 15. The architecture of a proof-of-concept prototype.

[16] https://polygon.technology

We assume that stakeholders' systems can be built on different blockchains such as Hyperledger, EOS, Ethereum, and Tezos. The orchestration layer enables the communication between these systems. The choreography layer integrates the different blockchain-based systems to enable the cross-organizational process. In our proof-of-concept, we use Polkadot[17] for integrating stakeholders; blockchains. Finally, when there is a conflict occurs in the cross-organizational process, it is propagated to the DAOs layer that implements the conflict resolution- and voting mechanisms.

5.2 Technology Stack

As in section 4.1, we have defined the system architecture and we proposed the usage of Ethereum smart contracts for patient, hospital, and healthcare professional systems and Polygon[18] smart contracts for insurance provider systems. For interoperability, we have proposed the usage of Polkadot. In the later sections, we have explained each of the selected technology and their working architecture.

5.2.1 Ethereum and Solidity

Ethereum is a decentralized open-source blockchain-based platform for smart contracts. It is a decentralized platform that creates a peer-to-peer network that securely executes and verifies a smart contract. Smart contracts are application codes that allow participants to perform transactions with each other without any dependency on a central authority. Some important components of Ethereum are the Ethereum virtual machine (EVM), miner, mining, transaction, block, account, consensus algorithm, smart contract, ethers, and gas.

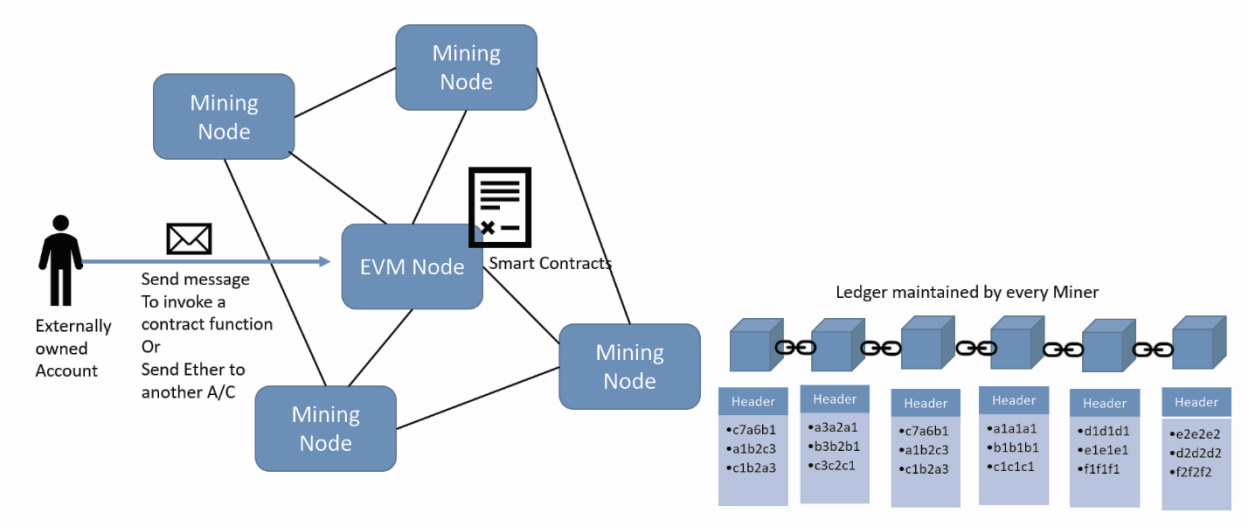

Figure 16. The architecture of Ethereum Blockchain [93]

[17] https://polkadot.network
[18] https://polygon.technology

A blockchain network consists of multiple nodes, nodes belonging to the miners. Nodes that are not used for mining are known as EVMs. Miners manage their instance of the ledger and in case if miner's instance is different from other miners sync with the latest (ongoing) block to keep data up to date. Each node is connected to another node on the network and uses a peer-to-peer protocol to communicate with each other [93].

5.2.2 Solidity

Solidity is the dominating object-oriented programing language that is used to write smart contracts for the Ethereum blockchain [94]. Solidity developed for Contracts maintains multiple members of variables to represent and arrangements. It carries out multiple types of supporting roles through the expediting Application Binary Interface and allows a secure and reliable process for different platforms involved in settlement or agreement between two entities.

Solidity is statically typed and supports inheritance, libraries, and complex user-defined types among other features. Solidity can be used for voting, crowdfunding, blind auctions, multi-signature wallets, and many other applications[19]. Below given is a simple smart contract storage code using solidity, which is quite like C++ and python.

Sample[20]

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.4.16 <0.9.0;

contract SimpleStorage {
   uint storedData;

   function set(uint x) public {
      storedData = x;
   }

   function get() public view returns (uint) {
      return storedData;
   }
}
```

5.2.3 Polygon

Polygon (MATIC) is one of the most ambitious cryptocurrency projects in recent history, which has a high growth potential due to the increased demand for non-fungible tokens (NFT), various decentralized finance (Defi) projects built on it, a project that provides extremely scalable with high network speed for transactions. Polygon is one of the largest projects in the crypto industry, originally designed to make transactions on the Ethereum blockchain much faster and cheaper than on the main network. The Polygon network is designed, in essence, as a solution to the problems associated with the Ethereum blockchain, the problem of Ethereum gas fees, which include high

[19] https://soliditylang.org/
[20] https://docs.soliditylang.org/

transaction fees and general network congestion, while maintaining the security of the network. Polygon aims to stimulate the mainstream adoption of cryptocurrencies by solving many of the scalability issues found in many blockchain networks. However, the Polygon network is unique in that it offers a second layer (layer 2) solution, which means that instead of making transactions on the Ethereum network, Polygon processes them first. Two different types of chains can be built in the Polygon ecosystem: Offline chains and secure chains. Autonomous chains can have their consensus models and are therefore less secure than networks using the Ethereum consensus model, but more flexible. Secure chains can be secured directly by Ethereum or by validators in the Polygon ecosystem, making them more secure but less flexible than standalone chains. Polygon's network architecture is unique in that it gives developers the ability to mix and match different scaling features rather than choosing just one.

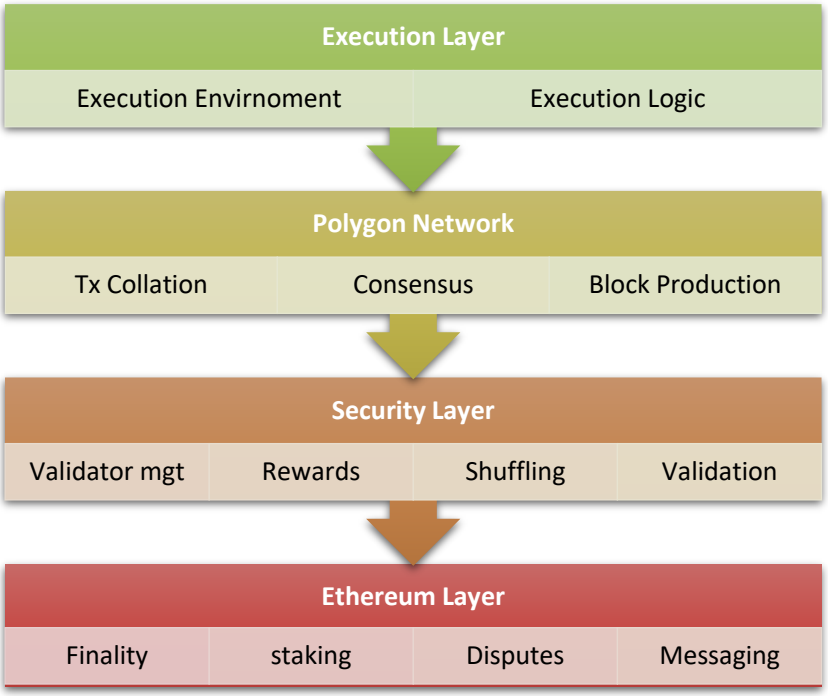

Figure 17. The architecture of Polygon

As Ethereum is used as the base layer for the Polygon chain, which provides high security but low flexibility. In the security layer, Polygon provides a "validator as a service" feature, allowing Polygon's validators to serve as chain consensus mechanisms. This is more flexible than using the Ethereum layer but slightly less secure. The polygon network layer consists of independent blockchain networks, where each network can support central functions, such as block creation and transaction matching. For a polygon project, this layer is required to build the project. The runtime layer is responsible for executing the transactions that run in the Polygon ecosystem. This is a required layer for a polygon-based project for execution. In our prototype, we use Polygon as it can overcome many of the barriers to scaling Ethereum with its unique framework that includes both scalability and backward compatibility while maintaining security and user-friendliness.

5.2.4 Polkadot

Polkadot is known as a "multi-chain network" that aims to connect various specialized blockchains into a single integrated network. Polkadot is a protocol that connects different blockchains and allows data to be sent over previously incompatible networks, for example. Bitcoin and Ethereum. Blockchains that connect to Polkadot operate in parallel as so-called "parachains". This allows them to access the transaction verification and security of the Polkadot network. The Polkadot network relies on proof of stake (PoS) to validate blocks. However, this is an oversimplification. There are three main roles in the Polkadot content network: collector, nominator, and validator.

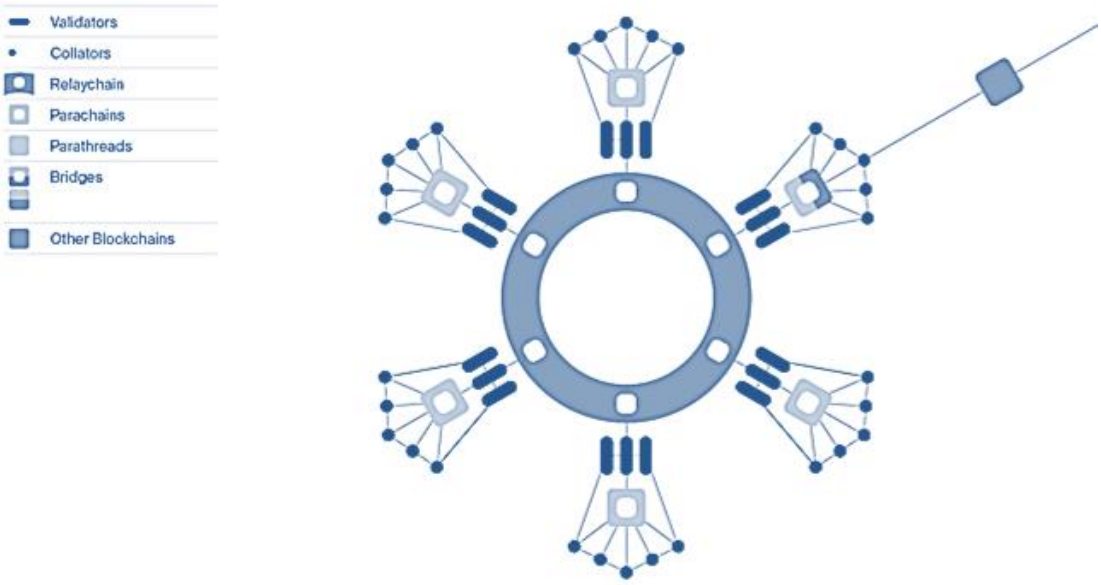

Figure 18. The architecture of Polkadot[21]

Figure 18 shows the architecture of the Polkadot network. Nominators are DOT token holders that choose the validators on the Polkadot network. They do this by staking (locking) their DOT with the validator of their choice and can gain new tokens for providing this service. Validators are objects that validate evidence provided by sorters on the network. They participate in consensus with other validators on the network by staking their DOT tokens and the tokens of the nominators who have chosen them. The network punishes unscrupulous players by reducing their DOT tokens and thus encourages fair verification. The matches collect transaction data from parachains and provide validators with proof that these calculations are correct. To do this, they maintain both a full parachain node and a relay chain.

[21] https://polkadot.network/

5.3 Conclusion

In this chapter, we mapped the defined techniques to the decentralized e-health systems. First, we defined the healthcare process with BPMN diagrams and propose multi-layered architecture. Next, we defined the technology stack for the implementation of the e-health privacy conflict resolution system. Finally, we proposed to implement DAO on the Ethereum blockchain.

In the first section, we use a model-driven engineering (MDE) approach defined in research [59] to create a well-tested smart-contract code.

The next section answers the first sub-research question (SRQ-1) which proposes the layered architecture of the proposed system. Layer one is an orchestration to enable the communication between patients and healthcare providers and healthcare professionals. Choreography is the second layer for the integration of different blockchain-based systems to enable the cross-organizational insurance process. In case of conflict in the choreography layer, we use a third layer based on Decentralized Autonomous Organization (DAO) which uses voting mechanisms as a conflict resolution technique to improve the performance of healthcare services.

The next section addresses the second sub-research question (SRQ-2) where we defined the technology stack for the implementation of the e-health privacy conflict resolution system. For the implementation of such a system in this research we propose to use smart contracts based on Ethereum, and polygon blockchains and to enable interoperability we propose to use polkadot.

To conclude this chapter, it can be said that the proposed architecture can be implemented using existing modeling techniques. From the proposed multi-layered architecture, it is possible to use blockchain for privacy conflict resolution in cross-organization processes in e-health. Also, it does not involve people in decision-making due to the usage of Decentralized Autonomous Organizations (DAO). However, an algorithm needs to be agreed upon and developed by people.

Due to time and scope constraints in this research we only used two different blockchains to resolve privacy conflicts however for future work, different blockchain networks will be tested to resolve privacy conflicts in various health applications, which are currently being used in the healthcare sector

6 Proof-of-concept prototype implementation

In this chapter, we will explain the implementation process for a proof-of-concept prototype. We have selected a running scenario to explain the end-to-end process which has been handled in the prototype for better understanding. Frist section 6.1 discusses the design and development of the prototype. Application flow and user interfaces for different users and application components are also explained in detail. Next, in section 6.2 research provides process evaluation using the formal Colored Petri Nets (CPN) model which aids to detect and eliminate design flaws and issues related to privacy and security. In next section 6.3, Research focuses on the formal conflict simulation and identification of different types of conflicts that occur when the stakeholders in the cross-organization process. Finally in section 6.4, state-space analysis for CPN models of the processes. The state-space analysis describes the behavior of the system, such as the absence of deadlocks, the possibility of always being able to reach a given state, and the guaranteed delivery of a given service.

6.1 Prototype Design and Development

In this research, we have proposed the design and development of a proof-of-concept prototype. This prototype has three major blockchain-based components. The first component is a patient app, which is used by the patients to add their medical health records. The second is the doctor's app where the doctor and patient health records. Finally, the third component is Health Insurance Provider. For implementation purposes, we have selected one scenario of adding a patient's blood pressure reading. The patient adds his blood pressure reading and saves it to the blockchain which is and then resolves the conflict

6.1.1 Patient App

Patient application is the first component of the prototype which is an interface provided for the patient to add his record. The application consists of the smart contract which is deployed to Ethereum Blockchain using Rospten test Network. A virtual MetaMask wallet browser extension is used which interacts with the Ethereum blockchain and allows to access the Ethereum wallet. To deploy our smart contract on the Testnet, we used fake ETH. For the Ethereum development environment, we used Hardhat which compiles smart contracts and runs them on a test development network. In the patient app, we have selected simple patient activity of adding blood pressure reading using the patient app. Following is the step-by-step flow of the patient application.

6.1.1.1 Adding Blood Pressure Reading

Figure 19 is the first screen where the patient can see his previously added blood pressure readings and input to add updated reading.

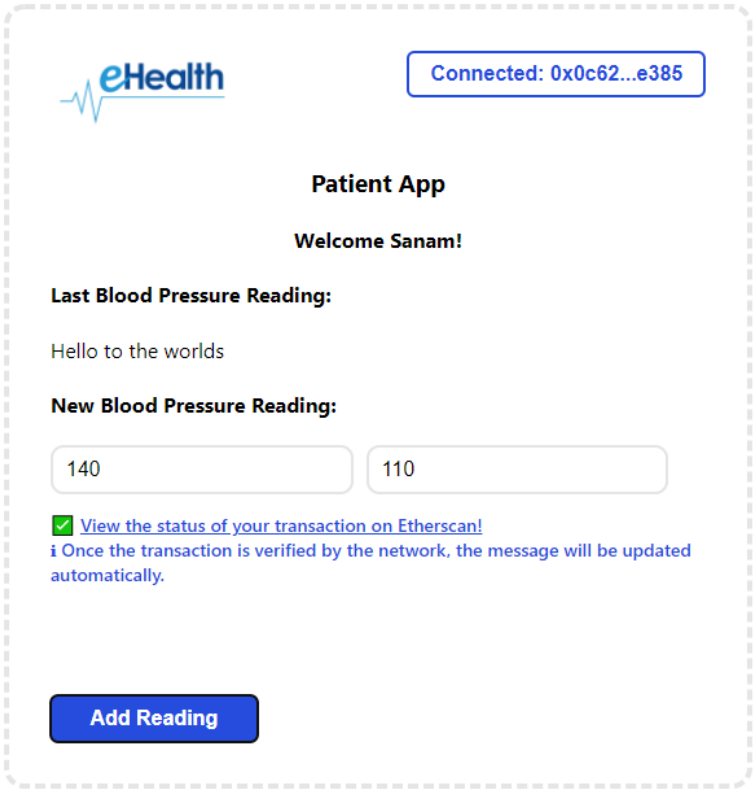

Figure 19. Patient App View - Adding Blood Pressure Reading

6.1.1.2 Confirmation of Posting Blood Pressure Reading

Once the user has connected the virtual wallet and confirmed the transaction after processing of transaction on the blockchain user can view the status and details on EhterScan.

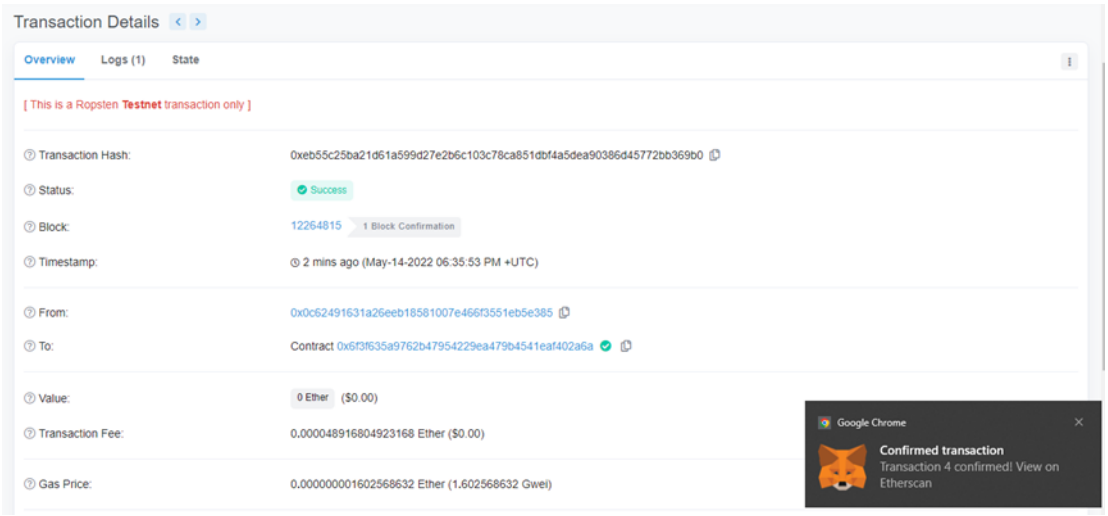

Figure 20. Patient App View - Confirmation of Posting Blood Pressure Record

6.1.1.3 Record Updated Confirmation

In the patient app, the user can also see the recently added blood pressure reading which confirms his record has been added successfully.

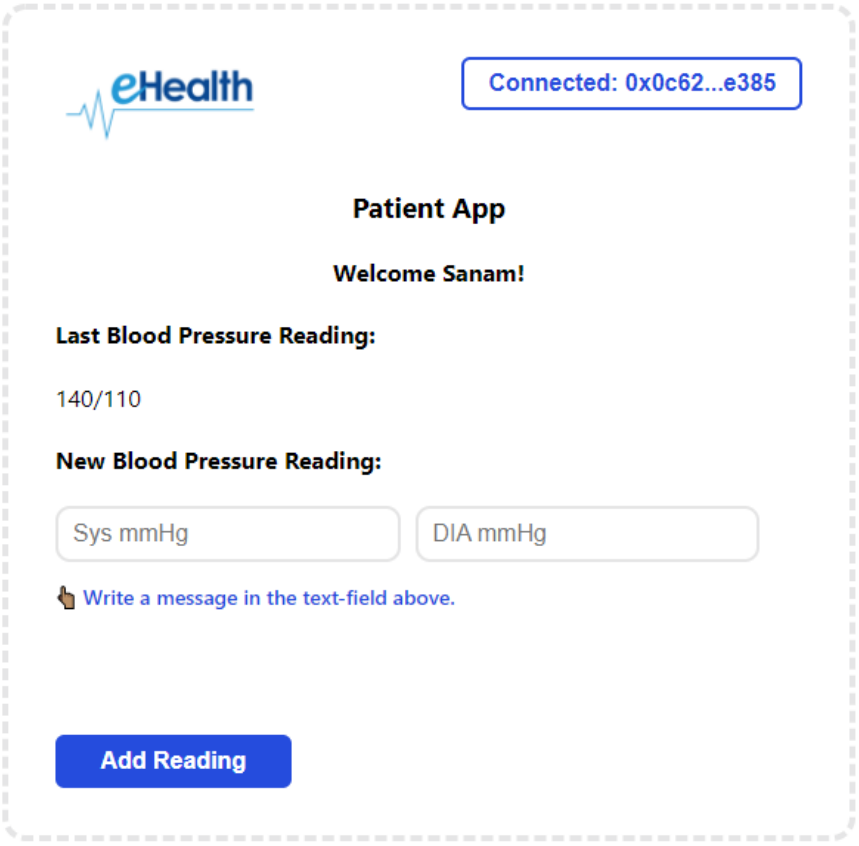

Figure 21. Patient App View - Posted Blood Pressure Reading

6.1.2 Doctor App

Doctor application is the second component of the prototype which is an interface provided to doctors to add patient records. The application consists of a smart contract that is deployed to Polygon Blockchain using Polygon Mumbai Testnet Network. Polygon is a framework and protocol which is used to build and compile blockchain networks that are Ethereum compatible. A virtual MetaMask wallet browser extension is used which interacts with the Polygon blockchain and allows to access the Polygon wallet. To deploy our smart contract on the Testnet, we used fake MATIC. For the development environment, we used Hardhat which compiles smart contracts and runs them on a test development network. In the doctor app, we have selected on simple doctor's activity of adding blood pressure reading for the patients using the doctor App. Following is the step-by-step flow of the doctor's application.

6.1.2.1 Adding Blood Pressure Reading

Figure 22 is the first screen where the doctor can see his previously added blood pressure readings for the patient and add updated readings.

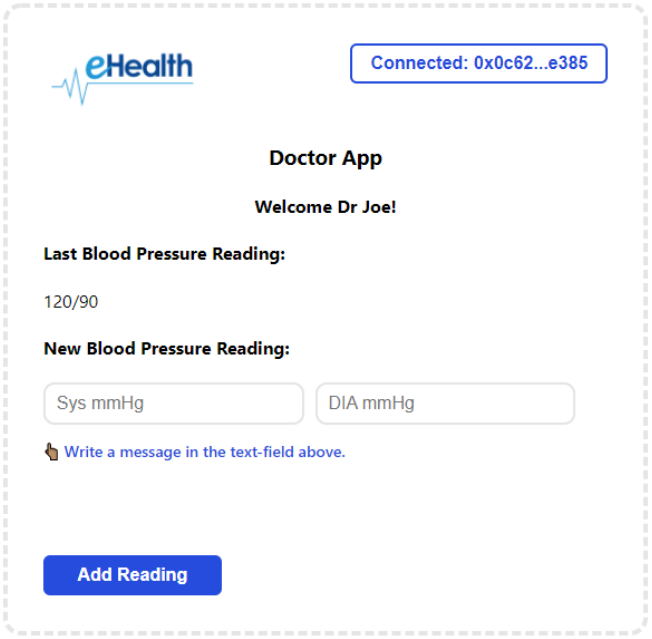

Figure 22. Patient App View - User's Last Record

6.1.2.2 Add New Blood Pressure Reading

Figure 23 shows the interface where the doctor adds new blood pressure readings.

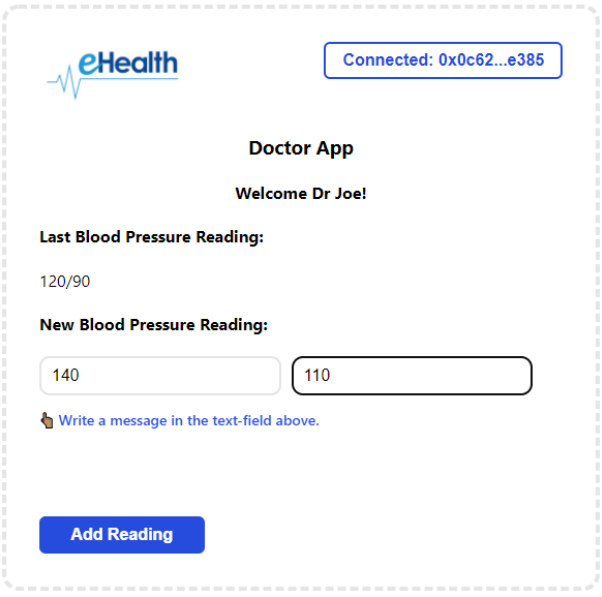

Figure 23. Doctors View - Add New Blood Pressure Reading

6.1.2.3 Wallet selection for Posting Transaction

Figure 24 shows the selection of accounts with Test MATIC and confirmation of readings.

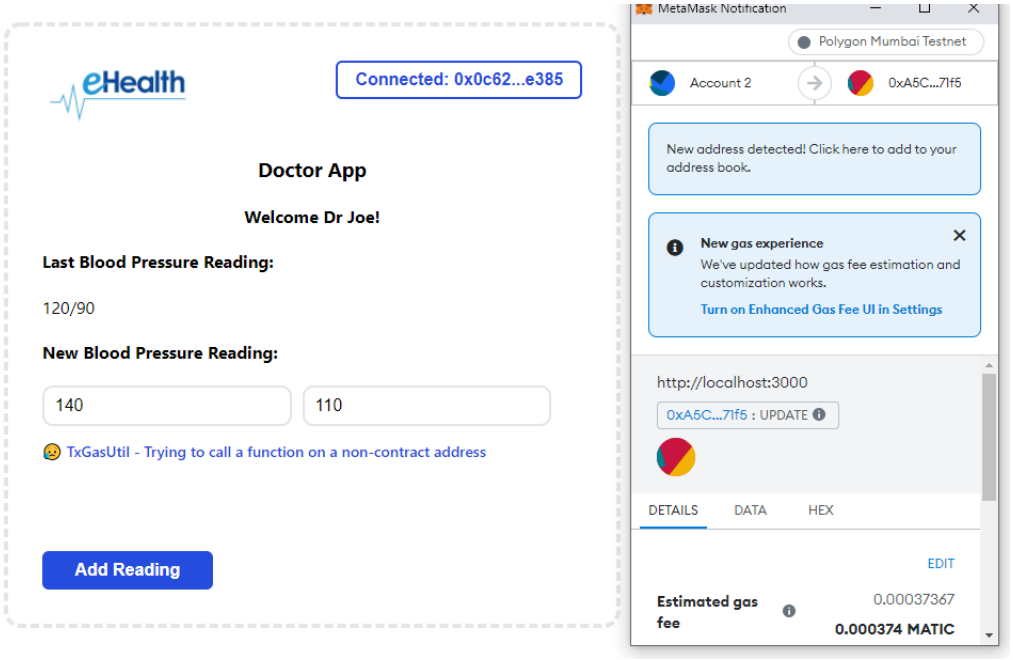

Figure 24. Doctor App View - Wallet selection for Posting Transaction

6.1.2.4 Confirmation of Posting Blood Pressure Reading

Once Doctor has connected the virtual wallet and confirmed the transaction, after processing of transaction on the blockchain user can view the status and details on the polygonscan.

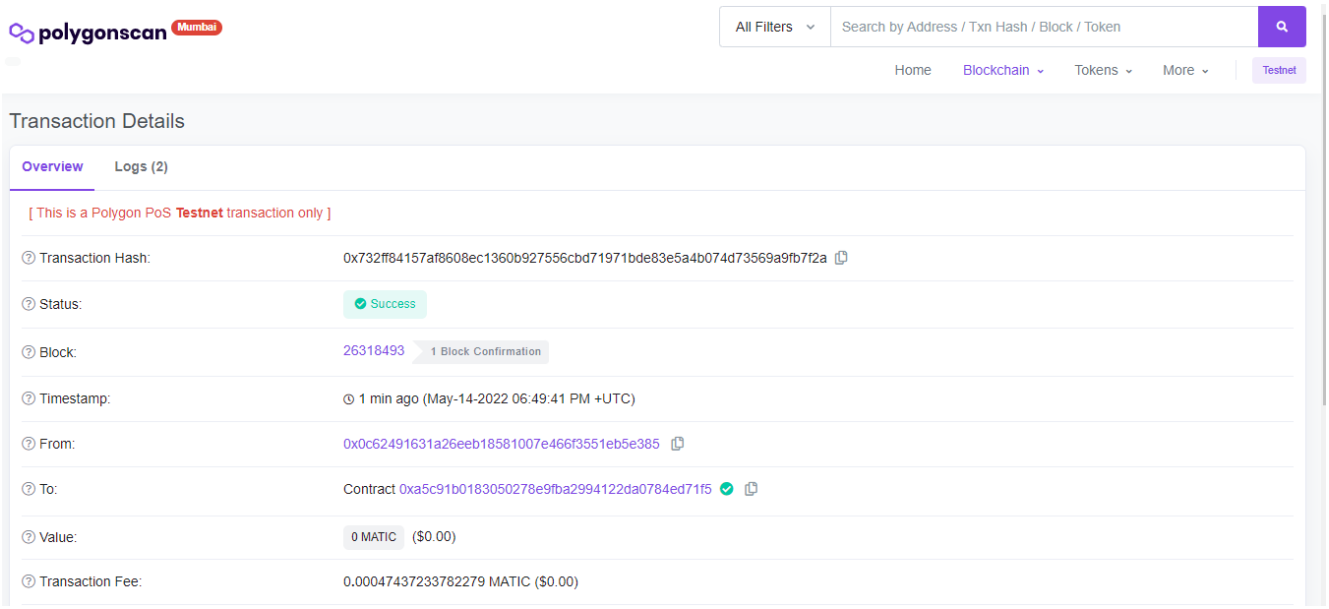

Figure 25. Doctor App View - Confirmation of Posting Blood Pressure Record

6.1.2.5 Record Updated Confirmation

In the doctor app, they can also see the recently added blood pressure reading which confirms the record has been added successfully.

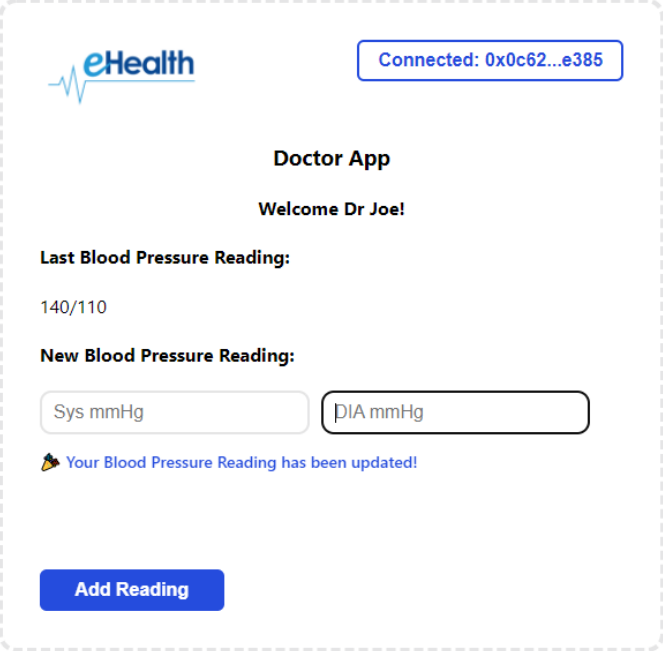

Figure 26. Doctor App- View - Posted Blood Pressure Reading

6.1.3 Healthcare Insurance Provider

The third component of the prototype is Healthcare Insurance Provider. As Polkadot uses parachain, which is an application-specific data structure. They introduced the concept of parallelized chains, which means they can parallelize the processing of the transaction and provide scalability to the Polkadot system.[22] We developed an application-specific blockchain-based module with the Substrate framework. Substrate SDK is selected to build the parachain for the healthcare insurance provider module. Substrate uses some predefined node template to create a blockchain network along with some predefined user accounts and balances.

The Healthcare Insurance Provider module runs as a backend local node. The interface for creating and deploying the contract is predefined when you use a substrate node template and create a contract project however, it is possible to update the contract according to the application needs. In this research, we used the default contract and updated it according to the running case of blood pressure readings.

[22] https://wiki.polkadot.network/docs/learn-parachains

6.2 Evaluation

For the evaluation of a provided privity-oriented PHR- and EHR integration process, we design a formal Colored Petri Nets (CPN) [86] model to detect and eliminate eventual design flaws, missing specifications, security, and privacy issues. We expand the collaboration scenario of Section 2.1 for a simulation using CPN so that also the conflict scenario is part of the quantitatively simulatable model. We evaluate our model in two ways. First, the original model is evaluated with simulation in CPN Tools, where we ensure that all initial tokens reach the unique end state of the model. Then, we perform the state-space analysis for the external layer of the model. The basic idea underlying state spaces is to compute all reachable states and state changes of the CPN model and represent these as a directed graph where nodes represent states and arcs represent occurring events. The state-space analysis describes the behavior of the system, such as the absence of deadlocks, the possibility of always being able to reach a given state, and the guaranteed delivery of a given service [88].

6.3 Formal Conflict Simulation

Table 1 lists the colors used for the collaboration scenario. There are two distinct parts to the CPN model. First, the External Layer shows how Patient, Healthcare professionals, and General practitioners collaborate in a cross-organizational environment when collecting medical data and providing it to the Insurance Provider. At the beginning of the collaboration, there is a process ID specified and represented as a p variable. Process ID identifies a collaboration case in the External Layer where the conflict occurs. In the Conflict Management Layer communication between different agents solving the conflict is shown. In the CPN model, there are five agents as Insurance Agent, General Practitioner Agent, Healthcare Professional Agent, Patient Agent, and Broadcast Agent. Agents propose claimer options such as patient, hospital, or healthcare professional. Agents have their internal business rules that define who is the claimer and if they have different opinions then they exchange the alternative opinions until reaching a consensus. If the decision of some agent needs to be propagated to more than one agent, then it is done by Broadcast Agent. The proposed claimers are represented by token colors such as pClaimer, gClaimer, hClaimer, and iClaimer. The alternative proposals have their token colors such as paClaimer, gaClaimer, haClaimer, and iaClaimer.

The second type of conflict occurs when the stakeholders in the cross-organization process provide the medical data collected from different data sources. The insurance provider prepares a claim based on blood pressure measurement in our running example and, thus, there should be only one measurement that all stakeholders agree with. The agents in the Conflict Management Layer manage the medical data conflicts as well as the claimer conflicts. The proposed values are represented with different token colors such as pmSuggested, gSuggested, pSuggested, and hpSuggested.

Color	Meaning
dataShared	Condition for sharing the personal data
dataExists	A condition that states if requested data is present or not
hSuggested	Blood pressure measurement suggested by the healthcare professional to be included in a claim
pgmt	Blood pressure measurement agreed upon by both patient and general practitioner
pmSuggested	Patient measurement proposed by Patient Agent after conflict resolution
gSuggested	Blood pressure measurement suggested by the general practitioner to be included in a claim
pSuggested	Blood pressure measurement suggested by the patient to be included in a claim
hpSuggested	Healthcare provider measurement proposed by Healthcare Provider Agent after conflict resolution
gmSuggested	General practitioner measurement proposed by General Practitioner Agent after conflict resolution
pPriority	Patient's priority for the claimer claim type
pClaimer	Claimer defined by the patient
gClaimer	Claimer defined by the general practitioner
hClaimer	Claimer defined by the healthcare professional
iClaimer	Claimer defined by the insurance provider
paClaimer	Claimer alternative defined by the patient
gaClaimer	Claimer alternative defined by the general practitioner
haClaimer	Claimer alternative defined by the healthcare professional
iaClaimer	Claimer alternative defined by the insurance provider

Table 1. Colors in the CPN model

Due to page limitations, we split the overall CPN model and present here patient-, healthcare provider, and general practitioner process snippets of the running case. The process snippets are implemented as subpages in the CPN model. Each internal process has an entry state called Start and an end state called End. The simplified internal business processes of Patients, General practitioners, and Healthcare professionals connect with the business process of Insurance providers through ports (places) labeled with Pat start, Pat out, GP start, GP out, H start, and H out. These places conceptually map so-called conjoint states.

For adhering to the WF-net formalism in CPNs, we use the token p from Table 1 as process ID for identifying a one case instantiating. Blood pressure measurement, as well as a proposed claimer for the insurance provider, join as additional token colors ranked behind p to form an external color tuple. In the CPN model, we express databases supplying process data as additional places. Differently to places of WF-net and the conjoinment places that cannot contain more than one token at a time belonging to the same process, places expressing database have no boundedness limitations with the second part of the CPN model on a higher hierarchy level as explained below, port places are needed in the WF-net. The second part of the CPN model, in Figure XX, on a higher hierarchy level interfaces through the port places with the lower level where the WF- net-based service collaboration resides.

This second higher level comprises five model-subsets that map a real-life system instantiation to conflict-management agents. The following sections describe the internal data collection processes and claimer definition for the patient, general practitioner, and healthcare professional.

6.3.1 Patient Internal Process

The internal patient data collection and claimer definition process are shown in Figure 19. When the insurance provider prepares a claim, he asks the patient to provide the blood pressure measurement. We assume that patient uses some application where his data is stored. First, the patient checks if the required data exists in his PHR and, if not, measures his blood pressure and saves it in the system. Next, the patient retrieves the data from the system and, if data can be shared with others, shares it with the insurance provider. For the simple reason, we do not consider the processing of PHR that cannot be shared, also, the data privacy policy can be different from system to system and is out of the current research scope. There is a business rule for the patient's decision of a claimer in the process defining the patient as a claimer if the blood pressure value is less than 160 and the hospital in the other case.

6.3.2 Healthcare Provider Internal Process

The internal general practitioner data collection and claimer definition process are shown in Figure 19. When the insurance provider prepares a claim, he asks the general practitioner to provide the blood pressure measurement. In the case of a general practitioner, we assume that he has access only to EHR as this data is gathered and managed by healthcare providers.

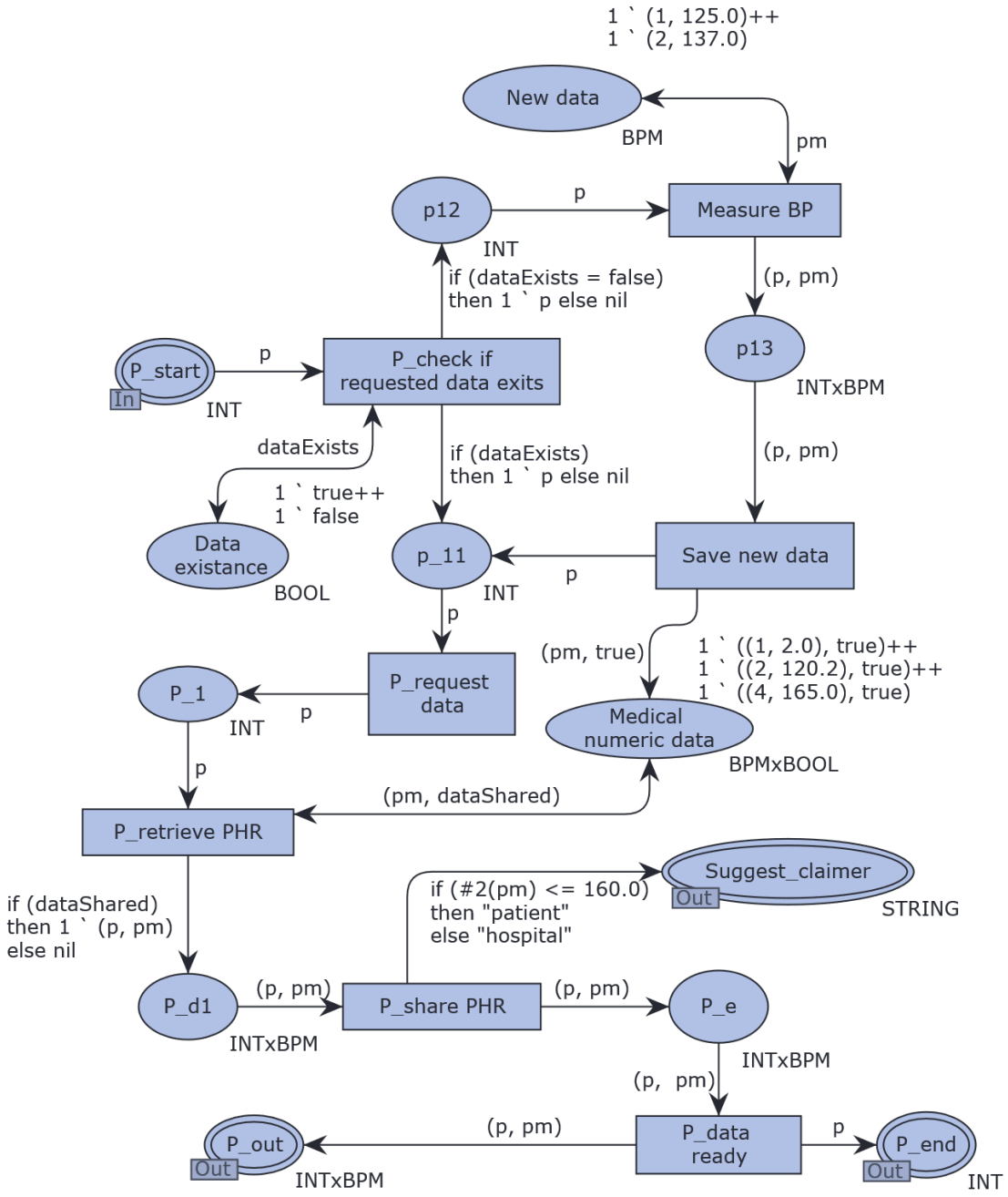

Figure 27. Healthcare provider internal process snippet of the running case

First, the general practitioner retrieves medical data from external systems. These can be other hospital systems or the national system that general practitioners have access to. Next, external EHR data is converted to the internal standard of the general practitioner's system and saved. After the data is saved, it is retrieved for sharing with the insurance provider. Again, we omit the data privacy setup process and consider sharing data with the insurance provider. The claimer is defined according to the general practitioner business rule defined in Figure 20: if blood pressure measurement is less or equal to 120, then the patient is defined as a claimer and otherwise hospital.

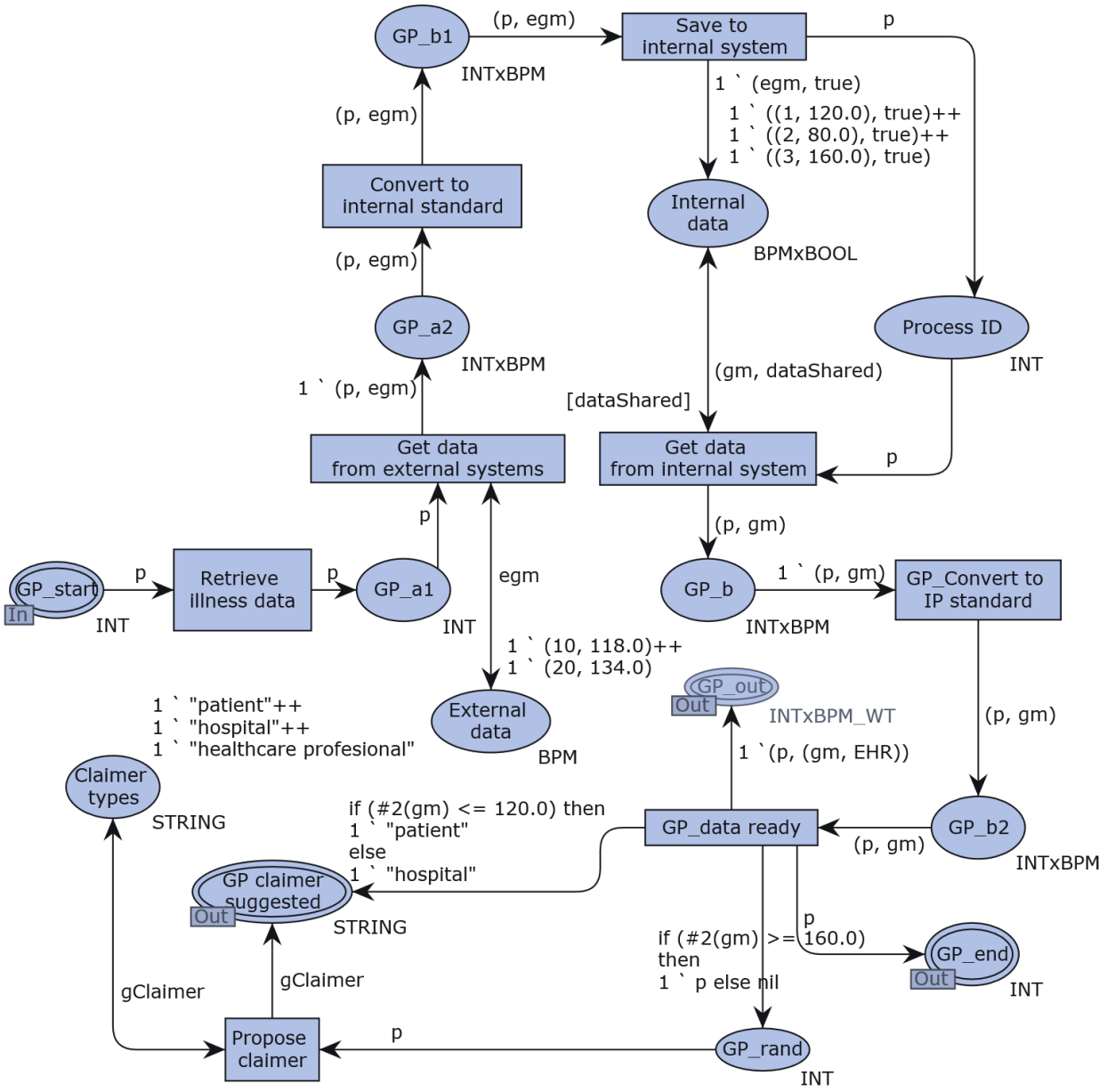

Figure 28. Healthcare provider internal process snippet of the running case

6.3.3 Healthcare Professional Internal Process

The internal healthcare professional data collection and claimer definition processes are described in Fig. 21. When the insurance provider prepares a claim, he asks the healthcare professional to provide the blood pressure measurement. The healthcare professional has access to both PHR and EHR. We use the PHR and EHR integration process described in the previous paper [92] as a foundation for the healthcare professional internal process in the CPN model.

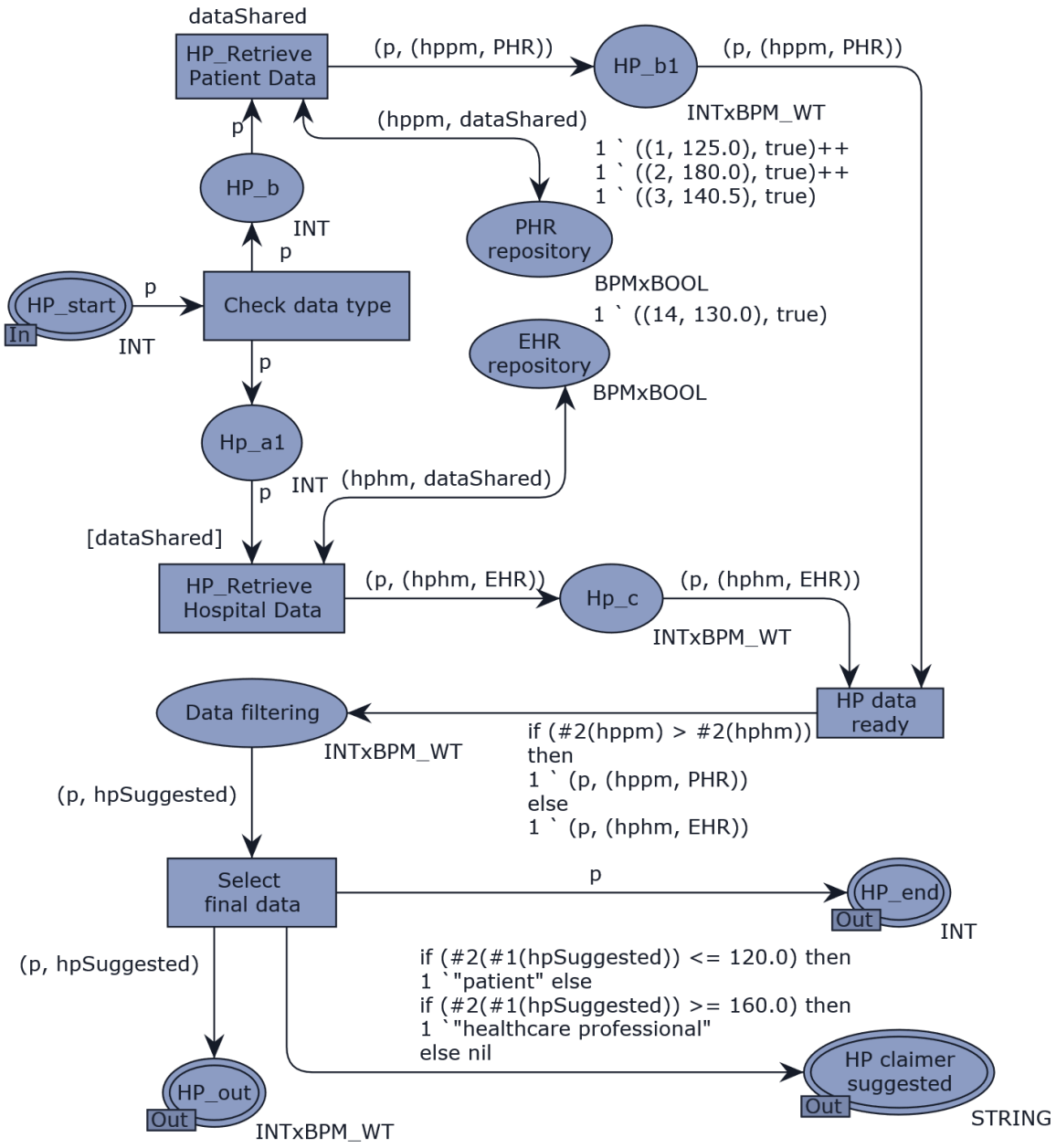

Figure 29. Healthcare professional internal process snippet of the running case

First, healthcare professional checks PHR and EHR repositories in parallel for the required data. We consider that data is shared according to the privacy regulations and leave the data-sharing mechanism out of scope in this thesis. When data is gathered, the noise data is filtered out. The validation for blood pressure measurement is based on the healthcare professional policy and is not detailed in this thesis. After filtering out noise data, the PHR or EHR is shared with the insurance provider. The healthcare professional defines the claimer according to the business rules defined in Figure 6. If blood pressure measurement is less than or equal to 120, the patient is defined as a claimer. If blood pressure measurement is more than or equal to 160, then a healthcare

professional is defined as a claimer. Business rules of the healthcare professional do not cover other measurement values.

6.4 State-Space Analysis

For evaluation, we performed state-space analysis for the external layer of the model which presents the state-space analysis results of the corresponding CPN models of the processes. The state-space analysis describes the behavior of the system, such as the absence of deadlocks, the possibility of always being able to reach a given state, and the guaranteed delivery of a given service [88]. The basic idea underlying state spaces is to compute all reachable states and state changes of the CPN model and represent these as a directed graph where nodes represent states and arcs represent occurring events.

While performing the state-space analysis, using the CPN model for all processes was used to calculate all the reachable states and state transitions. As we have limited process in this research which prevented state explosion and it was feasible to perform a full computational verification of the defined CPN model. After state calculation, a direct graph is presented, which contains nodes corresponding to the set of all reachable markings whereas arcs are linked to the occurring binding elements [95]. These graphs helped to derive all the properties of the CPN model and system. To perform the state-space analysis, we used the pre-built functionalities of CPN tools[23] . Based on the directed graph, we also calculated the Strongly Connected Components (SCC) graph which showed that there are 79 nodes and 84 arcs.

Loops	Home Markings	Dead Marking	Dead transitions	Live transitions
No	No	Yes	No	No

Table 2. State-Space Analysis for Evaluation

As shown in Table 2, there were no loops that represent the absence of infinite occurrences of the execution path and ensure the completion of the module. Also, from the result of the state-space analysis it can be seen there are no home markings. A Home marking is a marking that can be reached from any other reachable marking, which means that it is not possible to have a sequence of occurrences that cannot be extended to reach the home marking. Dead markings are detected in the analysis results and the cause is either customized input values or purposely deactivating some parts of the CPN Model that prevent a state-space explosion. The presence of dead marking ensures the completion/termination of executable action at a specified point which prevents infinite runtime. As the results indicate the presence of dead marking, so it is certain that there was no live transition. Live transition means we can always find an occurrence sequence that contains a transition from any reachable marking [95]. However, there are no dead transitions. A transition is dead if there is no reachable marking that allows the transition. Following are the details results

[23] http://cpntools.org/

for full state-space analysis which are available to view in the git repository mentioned in Appendix 9.2 and 9.3.

Boundedness Properties

Best Integer	Bounds	Upper	Lower
ExternalLayer'GP_end	1	1	0
ExternalLayer'GP_out	1	1	0
ExternalLayer'GP_start	1	1	0
ExternalLayer'HP_end	1	1	0
ExternalLayer'HP_out	1	1	0
ExternalLayer'HP_start	1	1	0
ExternalLayer'IP_a	1	1	0
ExternalLayer'IP_b	1	1	0
ExternalLayer'IP_c	1	1	0
ExternalLayer'IP_d	1	1	0
ExternalLayer'IP_e	1	1	0
ExternalLayer'IP_f	1	1	0
ExternalLayer'P_end	1	1	0
ExternalLayer'P_out	1	1	0
ExternalLayer'P_start	1	1	0
ExternalLayer'Uniqueue_end	1	1	0
ExternalLayer'uniqueue_start	1	1	0
Healthcare_professional_internall_process'Data_filtering	1	1	0
Healthcare_professional_internall_process'HP_b	1	1	0
Healthcare_professional_internall_process'HP_b1	1	1	0
Healthcare_professional_internall_process'Hp_Bp_Measurements_from_hospital	1	1	1
Healthcare_professional_internall_process'Hp_Bp_Measurements_from_patient	1	1	1
Healthcare_professional_internall_process'Hp_a1	1	1	0
Healthcare_professional_internall_process'Hp_c	1	1	0
Healthcare_provider_internal_process'External_data	1	1	1
Healthcare_provider_internal_process'GP_a	1	1	0
Healthcare_provider_internal_process'GP_a1	1	1	0
Healthcare_provider_internal_process'GP_a2	1	1	0
Healthcare_provider_internal_process'GP_b	1	1	0
Healthcare_provider_internal_process'GP_b1	1	1	0
Healthcare_provider_internal_process'GP_b2	1	1	0
Healthcare_provider_internal_process'Internal_data	1	2	1
Healthcare_provider_internal_process'Process_ID	1	1	0
Patient_internal_process'Data_existance	1	2	2

Patient_internal_process'New_data	1	1	1
Patient_internal_process'PHR_Repository	1	2	1
Patient_internal_process'P_1	1	1	0
Patient_internal_process'P_d1	1	1	0
Patient_internal_process'P_e	1	1	0
Patient_internal_process'p12	1	1	0
Patient_internal_process'p13	1	1	0
Patient_internal_process'p_11	1	1	0

Table 3. State-Space Analysis Results of Boundedness Properties

Upper Multiset Bounds

Best	Upper	Multi-set	Bounds
ExternalLayer'GP_end	1	1`1	
ExternalLayer'GP_out	1	1`(1,((1,120.0),EHR))++	1`(1,((10,118.0),EHR))
ExternalLayer'GP_start	1	1`1	
ExternalLayer'HP_end	1	1`1	
ExternalLayer'HP_out	1	1`(1,((14,130.0),EHR))	
ExternalLayer'HP_start	1	1`1	
ExternalLayer'IP_a	1	1`1	
ExternalLayer'IP_b	1	1`(1,((1,2.0),PHR))++	1`(1,((1,125.0),PHR))
ExternalLayer'IP_c	1	1`(1,((1,2.0),PHR))++	1`(1,((1,125.0),PHR))
ExternalLayer'IP_d	1	1`1	
ExternalLayer'IP_e	1	1`(1,((20,134.0),PHR))	
ExternalLayer'IP_f	1	1`1	
ExternalLayer'P_end	1	1`1	

ExternalLayer'P_out	1	1`(1,(1,2.0))++	1`(1,(1,125.0))
ExternalLayer'P_start	1	1`1	
ExternalLayer'Uniqueue_end	1	1`"claim"	
ExternalLayer'uniqueue_start	1	1`1	
Healthcare_professional_internall_process'Data_filtering	1	1`(1,((14,130.0),EHR))	
Healthcare_professional_internall_process'HP_b	1	1`1	
Healthcare_professional_internall_process'HP_b1	1	1`(1,((1,125.0),PHR))	
Healthcare_professional_internall_process'Hp_Bp_Measurements_from_hospital	1	1`((14,130.0),true)	
Healthcare_professional_internall_process'Hp_Bp_Measurements_from_patient	1	1`((1,125.0),true)	
Healthcare_professional_internall_process'Hp_a1	1	1`1	
Healthcare_professional_internall_process'Hp_c	1	1`(1,((14,130.0),EHR))	
Healthcare_provider_internal_process'External_data	1	1`(10,118.0)	
Healthcare_provider_internal_process'GP_a	1	1`(1,(1,120.0),true)++	1`(1,(10,118.0),true)
Healthcare_provider_internal_process'GP_a1	1	1`1	
Healthcare_provider_internal_process'GP_a2	1	1`(1,(10,118.0))	
Healthcare_provider_internal_process'GP_b	1	1`(1,(1,120.0))++	1`(1,(10,118.0))

Healthcare_provider_internal_process'GP_b1	1	1`(1,(10,118.0))	
Healthcare_provider_internal_process'GP_b2	1	1`(1,(1,120.0))++	1`(1,(10,118.0))
Healthcare_provider_internal_process'Internal_data	1	1`((1,120.0),true)++	1`((10,118.0),true)
Healthcare_provider_internal_process'Process_ID	1	1`1	
Patient_internal_process'Data_existance	1	1`false++	1`true
Patient_internal_process'New_data	1	1`(1,125.0)	
Patient_internal_process'PHR_Repository	1	1`((1,2.0),true)++	1`((1,125.0),true)
Patient_internal_process'P_1	1	1`1	
Patient_internal_process'P_d1	1	1`(1,(1,2.0))++	1`(1,(1,125.0))
Patient_internal_process'P_e	1	1`(1,(1,2.0))++	1`(1,(1,125.0))
Patient_internal_process'p12	1	1`1	
Patient_internal_process'p13	1	1`(1,(1,125.0))	
Patient_internal_process'p_11	1	1`1	

Table 4. State-Space Analysis Results for Upper Multi-set Bounds

Lower Multiset Bounds

Best	Lower	Multi-set	Bounds
ExternalLayer'GP_end	1	empty	
ExternalLayer'GP_out	1	empty	
ExternalLayer'GP_start	1	empty	

ExternalLayer'HP_end	1	empty	
ExternalLayer'HP_out	1	empty	
ExternalLayer'HP_start	1	empty	
ExternalLayer'IP_a	1	empty	
ExternalLayer'IP_b	1	empty	
ExternalLayer'IP_c	1	empty	
ExternalLayer'IP_d	1	empty	
ExternalLayer'IP_e	1	empty	
ExternalLayer'IP_f	1	empty	
ExternalLayer'P_end	1	empty	
ExternalLayer'P_out	1	empty	
ExternalLayer'P_start	1	empty	
ExternalLayer'Uniqueue_end	1	empty	
ExternalLayer'uniqueue_start	1	empty	
Healthcare_professional_internall_process'Data_filtering	1	empty	
Healthcare_professional_internall_process'HP_b	1	empty	
Healthcare_professional_internall_process'HP_b1	1	empty	
Healthcare_professional_internall_process'Hp_Bp_Measurements_from_hospital	1	1`((14,130.0),true)	
Healthcare_professional_internall_process'Hp_Bp_Measurements_from_patient	1	1`((1,125.0),true)	
Healthcare_professional_internall_process'Hp_a1	1	empty	
Healthcare_professional_internall_process'Hp_c	1	empty	
Healthcare_provider_internal_process'External_data	1	1`(10,118.0)	

Healthcare_provider_internal_process'GP_a	1	empty	
Healthcare_provider_internal_process'GP_a1	1	empty	
Healthcare_provider_internal_process'GP_a2	1	empty	
Healthcare_provider_internal_process'GP_b	1	empty	
Healthcare_provider_internal_process'GP_b1	1	empty	
Healthcare_provider_internal_process'GP_b2	1	empty	
Healthcare_provider_internal_process'Internal_data	1	1`((1,120.0),true)	
Healthcare_provider_internal_process'Process_ID	1	empty	
Patient_internal_process'Data_existance	1	1`false++	1`true
Patient_internal_process'New_data	1	1`(1,125.0)	
Patient_internal_process'PHR_Repository	1	1`((1,2.0),true)	
Patient_internal_process'P_1	1	empty	
Patient_internal_process'P_d1	1	empty	
Patient_internal_process'P_e	1	empty	
Patient_internal_process'p12	1	empty	
Patient_internal_process'p13	1	empty	
Patient_internal_process'p_11	1	empty	

Table 5. State-Space Analysis Results for Lower Multi-set Bounds

6.5 Conclusion

In this chapter, for the formal validation of proposed novel architectural concepts, a Colored Petri Net model is provided covering privity-oriented PHR and EHR integration process. We used a formal Colored Petri Nets (CPN) model in two ways. First, to evaluate simulation in CPN Tools, where we ensure that all initial tokens reach the unique end state of the model. Then, we performed the state-space analysis for the external layer of the model. The evaluation results were satisfactory

which showed the absence of deadlocks and data leaks in the model. We just performed a formal evaluation we do not evaluate the prototype, in respect of user feedback and technical prospect and, we only mocked one scenario in the proposed prototype which leaves a space for future work to handle multiple running cases. And provide an evaluation of running cases. We do not consider the security layer and patent identifier in the prototype itself and do not support multiple patients and doctors also in a production-ready system in future work it needs to be added.

7 Conclusion

The main goal of this thesis was to define a blockchain-based technique that helps to resolve privacy conflicts in cross-organization processes for e-health systems. We have proposed a blockchain-based technique to resolve the privacy conflict in the cross-organizational process in the e-Health system. Previous research [96] proposes a blockchain-based health data exchange framework that adequately solves the access control problems related to critical data storage in the cloud. A permission-based blockchain system that only grants access to invited and therefore verified users. In addition, to ensure data provenance, auditing, and secure traceability of medical data, the authors use smart contracts and an access control mechanism in their other work [97] to effectively track data behavior and recall access to violating organizations upon data permission violations. Research [98] proposed a three-tier system: the data usage layer, the data management layer, and the data storage layer. Unlike the above papers where the cloud is the storage infrastructure, this paper proposes that the private blockchain plays the role of the cloud. In [99], transactions are used to convey instructions such as storing, querying, and sharing data. The authors combine blockchain and off-chain storage to create a privacy-focused identity management platform. Research [96], provides a review of the latest biomedical/health applications of blockchain technologies and discusses potential challenges and proposed solutions for implementing blockchain technologies in the biomedical/health sector.

In contrast to the above works, which focus on health data sharing, [102] and [103] focus on other issues. Research [102] proposes a blockchain-based architecture for precision medicine and clinical trials. This paper explores blockchain-based system design starting from the medical field, specifically precision medicine and clinical.

Existing work provides various frameworks for healthcare personal data exchange in blockchain-based e-health systems. They consider blockchain as an auxiliary tool for data exchange, and not as a main for data storage, management, and exchange to resolve privacy conflicts. In addition, these works do not provide a detailed solution for privacy conflicts that arise while using this blockchain-based system in a cross-organizational process. We have proposed a blockchain-based technique to resolve the privacy conflict in the cross-organizational process in the e-Health system which has not been designed or developed in the previous research in this field.

7.1 Summary

To answer the main research question, we started with the identification of privacy conflicts in e-health cross-organizational processes. First, we defined disease prevention as the main process which can have possible privacy conflicts because of data exchange and communication among different systems i.e patient-, healthcare provider-, healthcare professional, and insurance. Next, we defined the requirements for conflict identification with the goal model and these requirements include insurance provision and transparently merging healthcare data. Then we defined data

collection conflict, transparency of internal processes to external stakeholders, integrity conflict across different processes, and data consistency conflict.

After identifying privacy conflicts in health cross-organizational processes, we proposed privacy resolution techniques. First, we perform a literature review of existing blockchain-based decentralized techniques in e-health systems which helps to resolve the privacy conflicts. Existing approaches include the usage of an architecture for a smart e-health gateway that not only reads but also processed the gathered medical data conflict-management lifecycle to provide a conflict resolution technique for virtual enterprises and defined conflict strategies which are the combination of conflict type and collaboration sub-patterns. Next, we define criteria for decentralized privacy resolution techniques with an ontology that describes contract-based business processes and includes conflicts together with their reasons (internal business rules) and possible consequences (remedies).

Finally, we map the defined techniques to the decentralized e-health systems. First, we defined the healthcare process with BPMN diagrams and propose multi-layered architecture. Layer one is an orchestration to enable the communication between patients and healthcare providers and healthcare professionals. Choreography is the second layer for the integration of different blockchain-based systems to enable the cross-organizational insurance process. In case of conflict in the choreography layer, we use a third layer based on Decentralized Autonomous Organization (DAO) which uses voting mechanisms as a conflict resolution technique. Next, we define the technology stack for the implementation of the e-health privacy conflict resolution system. For the implementation of such a system in this research we propose to use smart contracts based on Ethereum, and polygon blockchains and to enable interoperability we propose to use polkadot. Finally, we propose to implement DAO on the Ethereum blockchain.

For the formal validation of proposed novel architectural concepts, a Colored Petri Net model is provided covering privity-oriented PHR and EHR integration process. We used a formal Colored Petri Nets (CPN) model in two ways. First, to evaluate simulation in CPN Tools, where we ensure that all initial tokens reach the unique end state of the model. Then, we performed the state-space analysis for the external layer of the model. The evaluation results were satisfactory which showed the absence of deadlocks and data leaks in the model.

To conclude this research, it can be said that the extension of the goal model that has been done in this research is helpful to identify privacy-oriented processes and the development of blockchain-based e-health systems on a larger scale. Developing healthcare services requires privacy conflict resolution techniques. While identifying privacy conflicts usage of conflict resolution strategy previously used in Service-oriented cloud computing for virtual enterprises proved to be relevant in healthcare cross-organizational processes as well.

Unlike the traditional way of resolving privacy conflicts, Blockchain-based privacy conflict resolution techniques provide a decentralized and autonomous solution with a high degree of security, privacy, and performance. Healthcare cross-organizational domain acquires its ontology

that must be customized according to healthcare needs. Cross-organizational processes we need to have autonomous conflict resolution techniques based on different stakeholders, and goals.

From the proposed multi-layered architecture, it is possible to use blockchain for privacy conflict resolution in cross-organization processes in e-health. Different blockchains can be used for different sources of creating medical data by different stakeholders i.e patients, doctors, and healthcare providers. To provide interconnectivity and interoperability between different blockchains, Polkadot or similar platforms can be implemented according to the healthcare systems. Implementation of Decentralized Autonomous Organizations (DAOs) on the blockchain with predefined behavior and business rules in smart contract logic helps in decision making. Also, it does not involve people in decision-making due to the usage of Decentralized Autonomous Organizations (DAO). However, the algorithm needs to be agreed upon and developed by people.

7.2 Limitations

During this thesis research and development of the prototype, we had challenges and limitations related to blockchains as has decentralized nature of blockchain creates a new concept of a token economy where the community's income can be shared between real content producers and service users who create value. In this current research, we do not focus on token economy, so the aspects of token economy and transaction cost will not be covered. As maintaining privacy in user data is very important and failure to do this leads to implications related to legal sectors which are not covered in this research, so acceptance of proposed techniques depends on the country's legal law and hospital legal compliance. Due to the scope limitation of the master's thesis, an initial prototype will be prepared, however, this prototype will not the fully ready for production.

7.3 Future Work

Undoubtedly, there are several unsolved problems, starting with the legal aspects of implementing the systems and ending with the problems of technical compatibility and acceptance by people that need to be resolved in the coming years. The topics mentioned in the limitation e.g., what would be the token economy and how we can make it efficient? As posting data to blockchain is a transaction and it has a fee, the mechanism for who will get the money and who will pay how much money need to be designed in the future. As in our research, we have used different blockchains which means there will be different transaction fees for posting transactions on different blockchains i.e Ethereum and polygon. NFT and the voting mechanism is also not covered which leaves room for future work and improvements. Legal aspects related to the acceptance of smart contracts and compliance with GDPR, and other regulatory bodies are also a possible direction for future research. Future work will involve completing our ongoing implementation prototype and evaluating our approach to larger sets of processes and privacy conflicts in the e-health cross-organizational processes.

8 Bibliography

1. Beck, R., *Beyond bitcoin: The rise of blockchain world.* Computer, 2018. **51**(2): p. 54-58.
2. Aste, T., P. Tasca, and T. Di Matteo, *Blockchain technologies: The foreseeable impact on society and industry.* computer, 2017. **50**(9): p. 18-28.
3. Manzoor, A., et al. *A delay-tolerant payment scheme on the ethereum blockchain*. in *2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*. 2018. IEEE.
4. Brunese, L., et al., *A blockchain based proposal for protecting healthcare systems through formal methods.* Procedia Computer Science, 2019. **159**: p. 1787-1794.
5. McGhin, T., et al., *Blockchain in healthcare applications: Research challenges and opportunities.* Journal of Network and Computer Applications, 2019. **135**: p. 62-75.
6. Zhang, P., et al., *Blockchain technology use cases in healthcare*, in *Advances in computers*. 2018, Elsevier. p. 1-41.
7. Beinke, J.H., C. Fitte, and F. Teuteberg, *Towards a stakeholder-oriented blockchain-based architecture for electronic health records: design science research study.* Journal of medical Internet research, 2019. **21**(10): p. e13585.
8. Lea, N.C. and F. de Meyer, *How will the general data protection regulation affect healthcare?* Acta medica portuguesa, 2018. **31**(7-8): p. 363-365.
9. Susskind, R.E. and D. Susskind, *The future of the professions: How technology will transform the work of human experts*. 2015: Oxford University Press, USA.
10. Mercille, J., *Privatization in the Irish hospital sector since 1980.* Journal of Public Health, 2018. **40**(4): p. 863-870.
11. Hamza, R., et al., *A privacy-preserving cryptosystem for IoT E-healthcare.* Information Sciences, 2020. **527**: p. 493-510.
12. Kumar, P. and H.-J. Lee, *Security issues in healthcare applications using wireless medical sensor networks: A survey.* sensors, 2012. **12**(1): p. 55-91.
13. Kim, M.I. and K.B. Johnson, *Personal health records: evaluation of functionality and utility.* Journal of the American Medical Informatics Association, 2002. **9**(2): p. 171-180.
14. Chouhan, R., et al., *Lightweight Traceable Smart Health Care System using Cloud Computing.* 2018.
15. Chen, L., et al., *Blockchain based searchable encryption for electronic health record sharing.* Future generation computer systems, 2019. **95**: p. 420-429.
16. Gordon, W.J. and C. Catalini, *Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability.* Computational and structural biotechnology journal, 2018. **16**: p. 224-230.
17. Farouk, A., et al., *Blockchain platform for industrial healthcare: Vision and future opportunities.* Computer Communications, 2020. **154**: p. 223-235.
18. Codrin, A., *The Global "Blockchain in Healthcare" Report: the 2019 ultimate guide for every executive. Digital Disruption, May 26*. 2019.

19. Islam, N., et al., *A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services.* Future Generation Computer Systems, 2019. **100**: p. 569-578.
20. Chukwu, E. and L. Garg, *A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations.* IEEE Access, 2020. **8**: p. 21196-21214.
21. Syed, T.A., et al., *A comparative analysis of blockchain architecture and its applications: Problems and recommendations.* IEEE access, 2019. **7**: p. 176838-176869.
22. Esposito, C., et al., *Blockchain: A panacea for healthcare cloud-based data security and privacy?* IEEE Cloud Computing, 2018. **5**(1): p. 31-37.
23. Al Omar, A., et al., *Privacy-friendly platform for healthcare data in cloud based on blockchain environment.* Future generation computer systems, 2019. **95**: p. 511-521.
24. Christidis, K. and M. Devetsikiotis, *Blockchains and smart contracts for the internet of things.* Ieee Access, 2016. **4**: p. 2292-2303.
25. Hasselgren, A., et al., *Blockchain in healthcare and health sciences—A scoping review.* International Journal of Medical Informatics, 2020. **134**: p. 104040.
26. Xie, J., et al., *A survey of blockchain technology applied to smart cities: Research issues and challenges.* IEEE Communications Surveys & Tutorials, 2019. **21**(3): p. 2794-2830.
27. Liu, L.S., P.C. Shih, and G.R. Hayes, *Barriers to the adoption and use of personal health record systems*, in *Proceedings of the 2011 iConference*. 2011. p. 363-370.
28. Health, U.D.o. and H. Services, *Personal health records and the HIPAA privacy rule.* Washington, DC. URL: https://www. hhs. gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs. pdf [accessed 2016-06-20][WebCite Cache ID 6kLwH4Pzu], 2008.
29. Fernandez-Luque, L., R. Karlsen, and J. Bonander, *Review of extracting information from the Social Web for health personalization.* Journal of medical Internet research, 2011. **13**(1): p. e1432.
30. Tang, P.C., et al., *Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption.* Journal of the American Medical Informatics Association, 2006. **13**(2): p. 121-126.
31. Adida, B. and I.S. Kohane, *GenePING: secure, scalable management of personal genomic data.* BMC genomics, 2006. **7**(1): p. 1-10.
32. Abouelmehdi, K., A. Beni-Hessane, and H. Khaloufi, *Big healthcare data: preserving security and privacy.* Journal of big data, 2018. **5**(1): p. 1-18.
33. Archer, N., et al., *Personal health records: a scoping review.* Journal of the American Medical Informatics Association, 2011. **18**(4): p. 515-522.
34. Avizienis, A., et al., *Basic concepts and taxonomy of dependable and secure computing.* IEEE transactions on dependable and secure computing, 2004. **1**(1): p. 11-33.
35. Azorin-Lopez, J., et al., *Home technologies, smart systems and eHealth*, in *Mechatronic Futures*. 2016, Springer. p. 179-200.

36. Barr, E.T., et al., *The oracle problem in software testing: A survey.* IEEE transactions on software engineering, 2014. **41**(5): p. 507-525.
37. Becker, G., *Merkle signature schemes, merkle trees and their cryptanalysis.* Ruhr-University Bochum, Tech. Rep, 2008. **12**: p. 19.
38. Buterin, V., *A next-generation smart contract and decentralized application platform.* white paper, 2014. **3**(37).
39. Caldarelli, G., *Understanding the blockchain oracle problem: A call for action.* Information, 2020. **11**(11): p. 509.
40. Caldarelli, G. and J. Ellul, *The Blockchain Oracle Problem in Decentralized Finance—A Multivocal Approach.* Applied Sciences, 2021. **11**(16): p. 7572.
41. del Carmen Legaz-García, M., et al., *A semantic web based framework for the interoperability and exploitation of clinical models and EHR data.* Knowledge-Based Systems, 2016. **105**: p. 175-189.
42. Cilliers, L., *Wearable devices in healthcare: Privacy and information security issues.* Health information management journal, 2020. **49**(2-3): p. 150-156.
43. Damjan, M., *The interface between blockchain and the real world.* Ragion pratica, 2018(2): p. 379-406.
44. Davies, B. and J. Savulescu, *The right not to know: some steps towards a compromise.* Ethical Theory and Moral Practice, 2021. **24**(1): p. 137-150.
45. Dimitrov, D.V., *Medical internet of things and big data in healthcare.* Healthcare informatics research, 2016. **22**(3): p. 156-163.
46. Dittmar, A., et al. *Wearable medical devices using textile and flexible technologies for ambulatory monitoring*. in *2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*. 2006. IEEE.
47. Katurura, M. and L. Cilliers. *A review of the implementation of electronic health record systems on the African continent*. in *Proceedings of African Computer and Information System & Technology Conference*. 2017.
48. Hussein, A.F., et al., *A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform.* Cognitive Systems Research, 2018. **52**: p. 1-11.
49. Luo, E., et al., *Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems.* IEEE Communications Magazine, 2018. **56**(2): p. 163-168.
50. Zhang, P., et al., *FHIRChain: applying blockchain to securely and scalably share clinical data.* Computational and structural biotechnology journal, 2018. **16**: p. 267-278.
51. Sebestyen, G., et al. *eHealth solutions in the context of Internet of Things*. in *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*. 2014. IEEE.
52. Salehi, S. and M. Giacalone, *Conflict Resolution with Equitative Algorithms: A Tool to Establish A European Common Ground of Available Rights.* Conflict Resolution with Equitative Algorithms-A tool to establish a European Common Ground of Available

Rights", with S. Salehi, chapter of the book The European Common Ground of Available Rights, edited by F. Romeo, S. Martuccelli and M. Giacalone, Ed. Scientifica Napoli, 2019.
53. Xu, H., et al., *Conflict resolution using the graph model: strategic interactions in competition and cooperation*. 2018: Springer.
54. Neyens, G. *Conflict handling for autonomic systems*. in *2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W)*. 2017. IEEE.
55. Priya K, F. and N. Patil, *Resolving privacy conflict for maintaining privacy policies in online social networks.* International Journal of Computer Engineering and Technology, 2019. **10**(3): p. 94-101.
56. Agbo, C.C., Q.H. Mahmoud, and J.M. Eklund. *Blockchain technology in healthcare: a systematic review*. in *Healthcare*. 2019. Multidisciplinary Digital Publishing Institute.
57. Hölbl, M., et al., *A systematic review of the use of blockchain in healthcare.* Symmetry, 2018. **10**(10): p. 470.
58. Szabo, N., *Smart contracts: building blocks for digital markets.* EXTROPY: The Journal of Transhumanist Thought,(16), 1996. **18**(2): p. 28.
59. Sonsilphong, S., et al., *A semantic interoperability approach to health-care data: Resolving data-level conflicts.* Expert Systems, 2016. **33**(6): p. 531-547.
60. Narendra, N.C., et al., *Sound conflict management and resolution for virtual-enterprise collaborations.* Service Oriented Computing and Applications, 2016. **10**(3): p. 233-251.
61. Swan, M., *Blockchain: Blueprint for a new economy*. 2015: " O'Reilly Media, Inc.".
62. Nguyen, G.-T. and K. Kim, *A survey about consensus algorithms used in blockchain.* Journal of Information processing systems, 2018. **14**(1): p. 101-128.
63. Kormiltsyn, A., et al. *Improving healthcare processes with smart contracts*. in *International conference on business information systems*. 2019. Springer.
64. Udokwu, C., et al. *The state of the art for blockchain-enabled smart-contract applications in the organization*. in *2018 Ivannikov Ispras Open Conference (ISPRAS)*. 2018. IEEE.
65. Liu, L., et al., *From technology to society: An overview of blockchain-based dao.* IEEE Open Journal of the Computer Society, 2021.
66. Grefen, P., et al., *CrossFlow: Cross-organizational workflow management in dynamic virtual enterprises.* Computer Systems Science & Engineering, 2000. **1**(ARTICLE): p. 277-290.
67. Rahmani, A.-M., et al. *Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems*. in *2015 12th annual IEEE consumer communications and networking conference (CCNC)*. 2015. IEEE.
68. Leiding, B., *The M2X Economy-Concepts for Business Interactions, Transactions and Collaborations Among Autonomous Smart Devices*. 2019, Georg-August-Universität Göttingen.
69. Geels, F.W., *From sectoral systems of innovation to socio-technical systems: Insights about dynamics and change from sociology and institutional theory.* Research policy, 2004. **33**(6-7): p. 897-920.

70. Tsvetovat, M. and K.M. Carley, *Modeling complex socio-technical systems using multi-agent simulation methods.* KI, 2004. **18**(2): p. 23-28.
71. Antonopoulos, A.M. and G. Wood, *Mastering ethereum: building smart contracts and dapps*. 2018: O'reilly Media.
72. Shiang, C.W., J.-J. Meyer, and K. Taveter, *Agent-Oriented Methodology for Designing Cognitive Agents for Serious Games.* Engineering Multi-Agent Systems, 2016. **39**.
73. Norta, A., et al. *An agent-oriented method for designing large socio-technical service-ecosystems*. in *2014 IEEE World Congress on Services*. 2014. IEEE.
74. Sterling, L. and K. Taveter, *Art of Agent-oriented Modeling (Intelligent Robotics and Autonomous Agents)*. 2009: MIT Press.
75. Rossar, R., et al., *A Decentralized Insurance Marketplace on Blockchains for Achieving a High Level of Open Market-Information Symmetry (Version: 0.9 b).*
76. Sherkat, M., et al., *Emotional attachment framework for people-oriented software.* arXiv preprint arXiv:1803.08171, 2018.
77. Kormiltsyn, A., *A systematic approach to define requirements and engineer the ontology for semantically merging data sets for personal-centric healthcare systems.* 2018.
78. Sherkat, M., *Emotionalism in software engineering*. 2019, THE UNIVERSITY OF MELBOURNE: 2019.
79. Fulpagare Priya, K. and N.N. Patil, *Conflict Detection Techniques for Preserving Privacy in Social Media.* 2018.
80. Zhang, J., et al., *Data security and privacy-preserving in edge computing paradigm: Survey and open issues.* IEEE access, 2018. **6**: p. 18209-18237.
81. Gu, D., H. Li, and J. Zhang, *Software Engineering Data Modeling Based on OWL*. 2019.
82. Papež, V., S. Denaxas, and H. Hemingway. *Evaluation of semantic web technologies for storing computable definitions of electronic health records phenotyping algorithms*. in *AMIA Annual Symposium Proceedings*. 2017. American Medical Informatics Association.
83. Motik, B., R. Shearer, and I. Horrocks, *Hypertableau reasoning for description logics.* Journal of Artificial Intelligence Research, 2009. **36**: p. 165-228.
84. Allweyer, T., *BPMN 2.0: introduction to the standard for business process modeling*. 2016: BoD–Books on Demand.
85. Udokwu, C. and A. Norta, *Deriving and formalizing requirements of decentralized applications for inter-organizational collaborations on blockchain.* Arabian Journal for Science and Engineering, 2021. **46**(9): p. 8397-8414.
86. Morel, G., et al., *Manufacturing plant control challenges and issues.* Control Engineering Practice, 2007. **15**(11): p. 1321-1331.
87. Mahunnah, M., et al. *Heuristics for designing and evaluating socio-technical agent-oriented behaviour models with Coloured Petri Nets*. in *2014 IEEE 38th International Computer Software and Applications Conference Workshops*. 2014. IEEE.
88. Jensen, K. and L.M. Kristensen, *Coloured Petri nets: modelling and validation of concurrent systems*. 2009: Springer Science & Business Media.

89. Leiding, B., et al., *Authcoin: validation and authentication in decentralized networks.* arXiv preprint arXiv:1609.04955, 2016.
90. Westaway, M.D., P.W. Stratford, and J.M. Binkley, *The patient-specific functional scale: validation of its use in persons with neck dysfunction.* Journal of Orthopaedic & Sports Physical Therapy, 1998. **27**(5): p. 331-338.
91. Dwivedi, V., et al., *A formal specification smart-contract language for legally binding decentralized autonomous organizations.* IEEE Access, 2021. **9**: p. 76069-76082.
92. Kormiltsyn, A. and A. Norta. *Dynamically integrating electronic-with personal health records for ad-hoc healthcare quality improvements*. in *International Conference on Digital Transformation and Global Society*. 2017. Springer.
93. Modi, R., *Solidity Programming Essentials: A beginner's guide to build smart contracts for Ethereum and blockchain*. 2018: Packt Publishing Ltd.
94. Tikhomirov, S. *Ethereum: State of Knowledge and Research Perspectives*. 2018. Cham: Springer International Publishing.
95. Jensen, K., L.M. Kristensen, and L. Wells, *Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems.* International Journal on Software Tools for Technology Transfer, 2007. **9**(3): p. 213-254.
96. Kuo, T.-T., H.-E. Kim, and L. Ohno-Machado, *Blockchain distributed ledger technologies for biomedical and health care applications.* Journal of the American Medical Informatics Association, 2017. **24**(6): p. 1211-1220.
97. Xia, Q., et al., *MeDShare: Trust-less medical data sharing among cloud service providers via blockchain.* IEEE access, 2017. **5**: p. 14757-14767.
98. Yue, X., et al., *Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control.* Journal of medical systems, 2016. **40**(10): p. 1-8.
99. Zyskind, G. and O. Nathan. *Decentralizing privacy: Using blockchain to protect personal data*. in *2015 IEEE Security and Privacy Workshops*. 2015. IEEE.
100. Azaria, A., et al. *Medrec: Using blockchain for medical data access and permission management*. in *2016 2nd international conference on open and big data (OBD)*. 2016. IEEE.
101. Zhang, J., N. Xue, and X. Huang, *A secure system for pervasive social network-based healthcare.* Ieee Access, 2016. **4**: p. 9239-9250.
102. Shae, Z. and J.J. Tsai. *On the design of a blockchain platform for clinical trial and precision medicine*. in *2017 IEEE 37th international conference on distributed computing systems (ICDCS)*. 2017. IEEE.
103. Zhao, H., et al. *Lightweight backup and efficient recovery scheme for health blockchain keys*. in *2017 IEEE 13th international symposium on autonomous decentralized system (ISADS)*. 2017. IEEE.

9 Appendices

9.1 Access to Code Repository

Code of the prototype can be accessed using the git lab of Tartu University at the given below link:

https://gitlab.cs.ut.ee/nisar/privacyconflictresolutionbyblockchain

9.2 Access to Evaluation Results

Evaluation Results can be accessed using the git lab of Tartu University as given below link:

https://gitlab.cs.ut.ee/nisar/privacyconflictresolutionbyblockchain/-/blob/master/Evaluation%20Results/HealthInsurance_Evaluation_NoHierachy.cpn

9.3 Access to State-Space Analysis Results

https://gitlab.cs.ut.ee/nisar/privacyconflictresolutionbyblockchain/-/blob/master/Evaluation%20Results/SpaceStateAnalysisResults.txt

9.4 License

Non-exclusive license to reproduce thesis and make thesis public

I, **Sanam Nisar,**

1. herewith grant the University of Tartu a free permit (non-exclusive license) to reproduce, for preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   Defining blockchain-based techniques for privacy conflict-resolution in cross-organizational processes for e-health systems,

   supervised by: Aleksandr Kormiltsyn, Alex Norta, and Vimal Dwivedi.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons license CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.
3. I am aware of the fact that the author retains the rights specified on p. 1 and 2.
4. I certify that granting the non-exclusive license does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Sanam Nisar

14/05/2022