A Framework for Privacy and Security Requirements Analysis and Conflict Resolution for Supporting GDPR Compliance through Privacy-by-Design

Duaa Alkubaisy[1], Luca Piras[2], Mohammed Ghazi Al-Obeidallah[3],

Karl Cox[4], Haralambos Mouratidis [4 5]

[1] *Department of MIS, College of Applied Studies and Community Service, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia*
daalkubaisy@iau.edu.sa

[2] *School of Computing, Robert Gordon University, Aberdeen, UK*
l.piras@rgu.ac.uk

[3] *Faculty of Engineering, Al Ain University, United Arab Emirates*
mohamed.alobeidallah@aau.ac.ae

[4] *Centre for Secure, Intelligent and Usable Systems, University of Brighton, UK*
{K.Cox, H.Mouratidis}@brighton.ac.uk

[5] *Department of Computer and Systems Science, Stockholm University, Sweden*

Abstract. Requirements elicitation, analysis, and, above all, early detection of conflicts and resolution, are among the most important, strategic, complex and crucial activities for preventing software system failures, and reducing costs related to reengineering/fixing actions. This is especially important when critical Requirements Classes are involved, such as Privacy and Security Requirements. Recently, organisations have been heavily fined for lack of compliance with data protection regulations, such as the EU General Data Protection Regulation (GDPR). GDPR requires organisations to enforce privacy-by-design activities from the early stages and for the entire software engineering cycle. Accordingly, requirements engineers need methods and tools for systematically identifying privacy and security requirements, detecting and solving related conflicts. Existing techniques support requirements identification without detecting or mitigating conflicts. The framework and tool we propose in this paper, called ConfIs, fills this gap by supporting engineers and organisations in these complex activities, with its systematic and interactive process. We applied ConfIs to a realistic GDPR example from the DEFeND EU Project, and evaluated its supportiveness, with positive results, by involving privacy and security requirements experts[1].

[1] This research is an extension of the study conducted by Alkubaisy *et al.* [1] – which itself is a continuation of earlier studies [2,3] and aims to aid the reader in comprehensively grasping the concepts laid out.

Keywords: Security Requirements, Privacy Requirements, Requirements Conflicts, GDPR, Requirements Modelling, Privacy by Design.

1. Introduction

Today's software systems are seen to be susceptible to attack and performance issues due to matters regarding their inherent dependability [4], meaning their availability and reliability can come across as questionable. Especially considering the large amounts of sensitive and personal information kept on the servers of information systems, the security of such systems becomes even more important. The requirement engineering process of Software Engineering (SE) includes a variety of activities, from client contact through definition of requirements for the design. Since software is vulnerable to various threats, security, privacy, and trustworthiness have become important consideration in recent years [5]. Many contemporary SE paradigms are concerned with requirements; however, security, privacy, and trust implementations have received less attention. In practice, much emphasis is placed on incorporating security considerations throughout the coding and testing stages. Some paradigms handle these problems, but they only examine one of the three requirements: security, privacy, or trust, not all three at the same time. Hence, we think that security, privacy, and trust needs should be thoroughly collected, evaluated, and defined at different phases of the RE process.
Though, as important as system security is, privacy of the users must also always remain intact. This differentiation of security and privacy – and their respective requirements – should thus be given focused attention, both at the levels of understanding and at various stages of system development [6,7].

Every software system is characterized by its own security and privacy requirements, with the latter having become a bone of contention between many software developments companies, and their customers. Presumed misuse of personal data has garnered attention and action in the form of legislative controls to 'guarantee' privacy, especially as proposed by the EU's General Data Protection Regulation (GDPR) [8]. A common problem in the engineering process of software systems are conflicts arising between clashing requirements, such as privacy and security [9]. The nature of the software development process for realistic systems deems such conflicts inevitable and results in major inconsistencies [10]. Each requirement-based conflict is characterized by its own complex issues, understanding which is crucial to reaching their resolution [11]. Even in the presence of effective controls, such conflict may very well arise and adversely affect information systems [9,10,11,12]. Therefore, as

mentioned above, conflict identification earlier in the development lifecycle becomes even more crucial. This becomes more important for highly data-sensitive businesses such as banks and governmental departments which make up for almost 80% of all data breach incidents recorded [13].
GDPR has regulations in place to both educate citizens on how they can control where their data is used and to force organizations to have robust data usage and protection mechanisms in place. An example of the former is user consent while that of the latter is keeping track of the user data involved. The regulations enforced by GDPR can be difficult to put into actions, however. Once again, the inherent complexities in such measures resurface and add to the conflicts needed to be addressed. The approaches devised by literature in this area [14,15] seem to lack in-depth and applicable measures to identify and resolve the privacy-security conflicts, even though this identification and resolution, are crucial to minimize threats to the information system.
Considering this, the research questions (RQs) this paper will explore in the following sections are laid out as follows.

RQ1: How to design a framework supporting the analyst to identify and resolve conflicts between privacy and security requirements?
RQ2: How to support the analyst in the identification and resolution of conflicts between requirements in a systematic and tool-supported way in real cases?

Here, the requirement modelling tool SecTro [16,17] is extended to address **RQ1**. The resultant framework then offers an avenue of conflict identification and resolution for the analyst and is validated using the relevant portions of the DEFeND project [18] to ensure compliance with GDPR. For addressing **RQ2**, however, contemporary methods for conflict identification and resolution are reviewed and the novel ConfIS framework is introduced phase by phase to aid the analysts in the conflict location process.

The following sections will discuss the basis of the research conducted highlighting privacy and security requirements, and conflicting requirement likely to arise. Next a conflict resolution framework is proposed and DEFeND is used to answer RQ1. Afterwards, we address RQ2 by the extension of DEFeND to identify, resolve, and apply conflicts via the Tool Supported Conflict Resolution approach, followed by a case study and the assessing proposed ConfIS framework via expert group. Finally, we discuss the related work and concluding remarks.

2. Privacy and Security Requirements: Analysis and Conflict Resolution (State of the Art)

A system's capabilities at maintaining security and privacy can be gauged by the robustness of its respective requirements [19]. The successful satisfaction of these requirements then results in the minimization of conflicts and adherence to regulatory controls . This satisfaction becomes the ever-important factor while adopting a new system. At this point, analysts are supported in identifying security-privacy requirement conflicts and in subsequently resolving them. The proposed framework is a CASE Tool for Modelling Security in Requirements Engineering. The software Secure Tropos (SecTro) is used as it caters both to the needs of the users and the security requirements of the organization [20] while also ensuring that the resultant system is effectively defensive against cyber-attacks.

The benefits of this framework will allow the analyst to define and segregate privacy and security requirements. This enables the analyst to dive into the required level of detail in both these avenues and to make and understand their relationship with each other. Additionally, the framework enhances the understanding of software engineers regarding both security and privacy requirements and how they can harmonically coexist in a fully functional system. While the former caters to the organization's security policy, the latter are necessary to comply with data privacy laws and the issues that arise in balancing out them both must be identified and addressed as early in the development process as possible.

2.1 Conflicting Requirements

Conflicts are a part of almost every software system environment. These are inevitable and to have a smooth environment, they need to be terminated. The entire process of software development faces many inconsistencies and irregularities and one of the prime reasons for these instabilities is conflicting requirements. This problem occurs when a requirement is inconsistent with any another requirement. In this case, security and privacy requirements are mandatory but they have resulted in conflicting requirements. This is because multiple goals can have conflicting elements [21]. This conflict needs to be resolved, the entire process is dependent upon this resolution and this needs to be implemented on a business level to fulfill all the business needs.

While both privacy and security requirements hold their own significance, their coexistence can inevitably lead to conflicts. For example, the security requirement of authentication warrant's identity disclosure while the privacy requirement of anonymity opposes it. Another example can be taken from the case of data integrity versus unobservability, where the former necessitates tracking user activity across networks while the latter strongly resists it.
The security and privacy requirements come head-to-head once again in the battle of authentication. While data security entails the user to reveal as much information about their identity as possible to ascertain authenticity, the user privacy requirements of anonymity and pseudonymity require that the personally identifiable information of a user be as unavailable and protected as possible to reduce exposure. This conflict seems to take inspiration from real life and is faced in many a scenario. For instance, governments may be keen on collecting as much information about their citizens as possible in the interest of national security. Contrarily, citizens may have to live with concerns of privacy encroachment and may thus resist such observatory policies.

Additionally, privacy requirements bring with them concerns related to unobservability and Unlinkability. These two concerns act to severely impact the security requirements converse to them, but if the security requirements are given precedence, the privacy requirements would undeniably suffer. Such concerns help us envisage the sources of conflict in the security-privacy domain that need pertinent attention to be resolved appropriately. If not given due importance, such conflicts can prove to be detrimental to system stability. And while the nature of the conflicts remains similar, the idiosyncrasies of specific situations demand situation-specific attention.
The security requirement of authorization is another issue for potential conflict, as it is directly in contradiction to the privacy requirement of unobservability. In this, authorization demands the user to reveal themselves to the adequate degree while the preservation of privacy of the user requires concealment. This negotiation complicates the authentication cover of approval while also putting the user's identity in threat.

Consequently, a lot of aspects of privacy and security requirements seem to conflict with each other. The long list of an organization's security requirements including authenticity, accountability, non-repudiation, and auditability for record-keeping purposes, activity logs are required. In direct contrast, however, the concurrent privacy requirements like unobservability and anonymity be visible. Moreover, the actions of separation of duties (SoD) and binding of duties (BoD) act to further these conflicts as they lie in contradiction

to the privacy requirements of anonymity and Unlinkability as these comparative exercises demand the verification of identity of the involved parties.

Moreover, to identifying these conflicts at the requirements stage, there may be some aspects that become apparent at later stages in the (SDLC) Software Development Life Cycle. For instance, the intrinsic characteristics of the security requirements of integrity, confidentiality, and availability are dependent upon the act of authorisation itself, necessitating granting access or modifying resources. And while user identification is not necessary for these requirements, it may be the approach some developers employ. Consequently, this can lead to later-stage security-privacy requirement conflicts, especially when more concrete requirements must be considered. For instance, instead of requiring the user to access a service using their own identity, they can be given the leeway to sign in using an alias. However, since the alias is still a unique identity able to be attributed to the user, it again comes in conflict with the concept of anonymity. Nonetheless, if some aspects of privacy or security requirements supplement or overlap with aspects of the other, their conflicting characteristics may be able to be overlooked. For example, the requirements of integrity, anonymity, and confidentiality all aim towards the singular purpose of minimising data breaches, thereby acting in unison.

This section illustrates via visual maps, the most frequently conflicting requirements. Extending from literature, the five security requirements likely to conflict with multiple privacy requirements are depicted in Figure 1. The most conflicting security requirement is seen to be availability as it directly conflicts with four privacy requirements, namely Unlinkability anonymity, undetectability, and unobservability. The next most conflicting security requirements are accountability, confidentiality, and auditability, each conflicting with three privacy requirements. These are followed by authentication which conflicts with two privacy requirements.

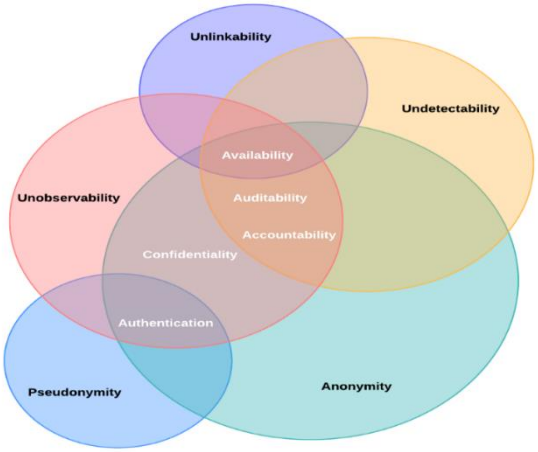

Fig. 1. Detecting conflicts between Security and Privacy Requirements (Venn diagram) (Alkubaisy et al., 2019)

It must be kept in mind that this list of security requirements is not exhaustive, but rather addresses the most common or frequently occurring and conflicting ones. Some security requirements are also not mentioned here since they do not seem to conflict with any privacy requirement.

2.2 Conflict Resolution - Framework and Process

The resolution process can give a clearer direction regarding other elements that were not previously discussed. This shows how prioritizing requirements is integral and which goal or element can be abandoned. This further highlight other important goals that can be achieved through this process. The overall change in business goals can alter the requirements, so the goals need to be achievable because if they are not achievable and realistic then the entire project can collapse.

The proposed framework has a sequence of phases to achieve conflict detection and resolution, presented in Figure 2:

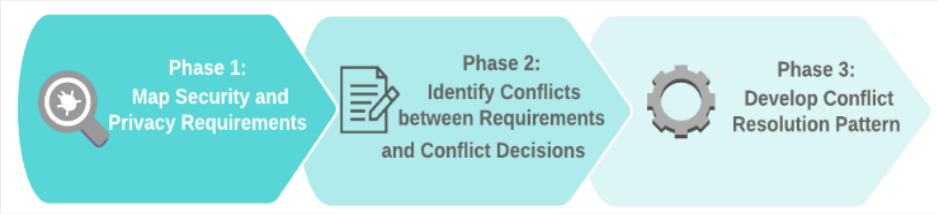

Fig. 2. The phases of the proposed theoretical framework- ConfIS Framework (Alkubaisy et al., 2021)

The framework process has a combination of manual and semi-automated steps. These are majorly based on the perspective of the analyst who formed the theoretical framework. A common perspective among all these. The first and foremost step is to identify and analyze the conflicts between the requirements. This is established upon the matrix of existing studies which helps in identifying the requirements that can be conflict. Moreover, the analyst considers impacts of the conflict on the system. The software requirement analyst performs this phase, which is the first phase manually.

Phase 1: Mapping Security and Privacy Requirements

The first step of detecting conflicts is to review the literature to determine more about conflicting issues. This provides some examples to detect how conflict affects a system. In the first phase, the existing literature is reviewed

to have a better understanding of the conflicts between requirements (Table 1). This can give some idea to the analyst regarding the impact of conflicts on specific systems. The matrix used in the identification helps map security requirements and privacy requirements. It is determined which conflicts exist between the two aspects.

Table 1. Most Frequent Security and Privacy Requirements being in Conflict

Security Requirements	Availability, Non-Repudiation, Confidentiality, Integrity, Authentication, AuthoriSation, Separation of duties (SoD), Binding of duties (BoD), Accountability, Auditability
Privacy Requirements	Anonymity, Unlinkability, Pseudonymity, Unobservability, Undetectability

Mapping Between Security and Privacy Requirements

The matrix maps conflicts between security requirements and privacy requirements. While there may indeed be conflicts among security requirements themselves, the matrix will focus on conflicts that cross the two aspects. The matrix helps us to visualize the requirements with the most conflicts, which aids in identifying which deserve focus. From this matrix, anonymity and unobservability conflict the most with other security requirements (Table 2).

Table 2. Mapping conflicts between Security and Privacy Requirements

		Security Requirements:										*Privacy Requirements:*				
		Availability	**Non repudiation**	**Confidentiality**	**Integrity**	**Authentication**	**Authorization**	**SOD**	**BOD**	**Accountability**	**Auditability**	**Anonymity**	**Unlinkability**	**Pseudonymity**	**Unobservability**	**Undetectability**
Security Requirements:	**Availability**							○				○	○		○	○
	Non repudiation											○			○	
	Confidentiality											○			○	
	Integrity											○	○		○	
	Authentication						○					○		○	○	
	Authorization					○		○							○	
	SOD	○					○									
	BOD												○	○		
	Accountability											○			○	○
	Auditability											○			○	○
Privacy Requirements	**Anonymity**	○	○	○	○	○				○	○	○	○	○	○	
	Unlinkability	○			○				○			○		○		○
	Pseudonymity					○			○			○	○			
	Unobservability	○	○	○	○	○	○			○	○	○				○
	Undetectability	○								○	○		○		○	

Phase 2: Identify Conflicts between Requirements and Conflict Decisions

When we maintain security or privacy requirements, several challenges arise, according to an analyst's perspective. As discussed earlier, conflicts and problems are inevitable. Developers find it necessary to manage the conflicts that arise in this process and be compliant with GDPR. Identification of conflicts is essential and to do that, we analyze different scenario tasks to address conflicts. An example is used to explain this phase. We have to identify conflict in a situation where older people need to be taken care of by obtaining their personal information. This comes with security risks. Integrity and anonymity are the two requirements being conflict. Anonymity is a privacy requirement, and integrity is a security requirement.

Therefore, a conflict can arise if both the requirements have to be satisfied. It is vital to maintain the anonymity of the patient information according to privacy-by Design principles. Moreover, integrity is also important because sensitive information is being shared. Now, the requirements are mapped, and conflict is identified which is between integrity and anonymity. The analyst needs to evaluate all the scenarios related to this issue and evaluate them individually. The security and privacy requirements will be evaluated separately, and conflicts will be analyzed. This will assist the analyst in progressing to the resolution phase with all of the required information.

Phase 3: Tool Supported Conflict Resolution Patterns

Eventually, different solutions are proposed to deal with the conflict requirements. Thus, each type of conflict is set aside, and a model of patterns is found to connect the conflicting requirements with a supporting tool (Figure 3). We need to find a tool that can satisfy both requirements without any sort of conflict. A relevant tool that can satisfy security and privacy requirements and resolve the conflict. The tool needs to be added to the Privacy Pattern Library for proper processing. The supporting tool needs to be added into the framework so that it is complete, and a conflict can be easily tackled through this tool.

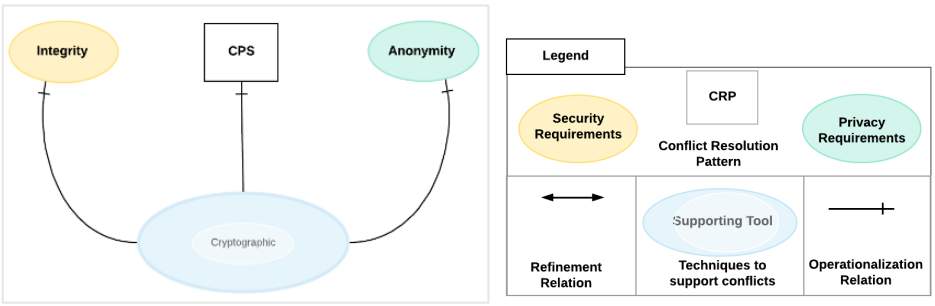

Fig. 3. Conflict Resolution Pattern (Alkubaisy et al., 2021)

3. DEFeND Project

Given the sensitivity of data and personal information organizations store of clients and customers, they are expected to comply with the European Union's General Data Protection Regulation (GDPR). DEFeND provides a platform to accredit organizations in different regions. This platform aims to have a plan to achieve GDPR compliance and raise awareness regarding its diverse features [22,23]. All the scenarios are taken into consideration by the ConfIS framework which was not resolved by DEFeND project previously. By applying this framework, many conflicts are resolved now. The focus was on Data Scope Management (DSM), Data Protection Impact Assessment (DPIA), Privacy by Design and Security, and Privacy Threats. This research uses healthcare scenarios (mentioned in Section 5) of DEFeND project because it was more relevant, and it focused on sensitive user information and the personal data of the patient. There was also the potential to map requirements and identify conflicts related to this. Furthermore, the platform and the framework majorly support in discovering security and privacy requirements, identifying conflicts, and proposing legitimate solutions.

4. ConfIS Integration and SecTro

The SecTro tool has been used to aid in the modelling of conflicts resolution [1]. It implements the Secure Tropos Methodology which consists of an engineering approach for security and privacy requirements, starting from early-stage requirements of the (IS) Information System development process. Secure Tropos must be specified in the early phases of an IS development, as it is an organized approach for goal-oriented security and privacy requirement modelling. The Secure Tropos methodology supports a modelling language, security aware processes and automated processes. In fact, Secure Tropos methodology enhances our framework by translating conflicts between requirements in a goal model. SecTro presents models that contain security and privacy requirements [22]. It involves modelling views which are used to facilitate system design and elicitation of security and privacy requirements.

5. Motivation Scenario

There are a variety of scenarios where the conflicts arisen between security and privacy requirements can be seen to be exemplified. Neither one's respective significance can be ignored; however, each scenario accordingly demands individual attention. In our case study- Doctor and Patient, we have used the ConfIS framework on the DEFeND platform that aims to achieve conflict resolutions [23]. For maintaining confidentiality of Patient's record to avoid data breaches, a monitoring system must be installed in the hospitals. Another reason for installing a monitoring system is to remain in compliance with GDPR's regulations particularly when Third Parties are involved, for example external laboratories. For securing patient's data: The DEFeND platform introduces risk assessment, and Data Protection Impact Assessments (DPIA) along with validation process and proposed GDPR plan. A graphical representation of the model is achieved by the Hospital Analyst supporting doctors being able to change medical records by adding results from external parties (laboratories) and achieving approval from supervisors [24]. Furthermore, the DEFeND platform works with the organizational structure of the hospital, keeping hierarchy, and their interactions in check. The system comes with a configuration model for monitoring threats identified after Data Protection Impact Assessment (DPIA), Self-assessment, and related models for identifying potential threats.

The theoretical framework is built on the SecTro tool. Our case study in Phase 1 is supported by diagrams, and Privacy by Design tool to resolve conflicts. Phase 2 will identify security and privacy conflicts between these parties. The hospital analyst is supposed to make a sound decision based on the content of the identified conflict. In Phase 3, all concepts are added together, and solutions are presented to mitigate the identified conflict. After all of this, a case study is presented which implements all these three phases for an in-depth study. In Phase 1 to 3, ConfIS framework is introduced.
Based on the motivation example, we will illustrate the security and privacy requirements, following the phases of the ConfIS framework to resolve conflicts, using the extended supported tool. The first phase aims to map the security and privacy requirements [2]. This assumes the existence of a matrix to find out the potential conflicts between security and privacy requirements,

based on our recent study [18]. The next sections show the application of our proposed framework phases in identifying and resolving conflicts, discusses the application of the motivation example in SecTro, and presents the theoretical framework to identify and resolve conflicts

Phase 1: Mapping Security and Privacy Requirements

The privacy and security conditions are implicated in the determination of conflicts using a Mapping Matrix. To find out the reason for conflicting requirements, we have formed an outline by using Figure 4 where the organization view of SecTro is exhibited. In the given flowchart each bubble depicts an actor which in our examples are doctor, supervisor, and an employee. To identify conflicts we have split the scenario to specify certain tasks to actors (doctor, employee, and supervisor). The tasks specified to them have distinct and precise requirements. The doctor requires medical history, data, and results from an Employee the main concern here is the privacy and integrity to send such confidential data, so the patient's privacy is not breached at any cost. Additionally, the data that is recorded after the doctor's careful examination or the update of a patient's medical record in the system should always be confidential. At the same time, the data recorded by the doctor needs to be authenticated by the supervisor. The long chain of action demands responsibility.

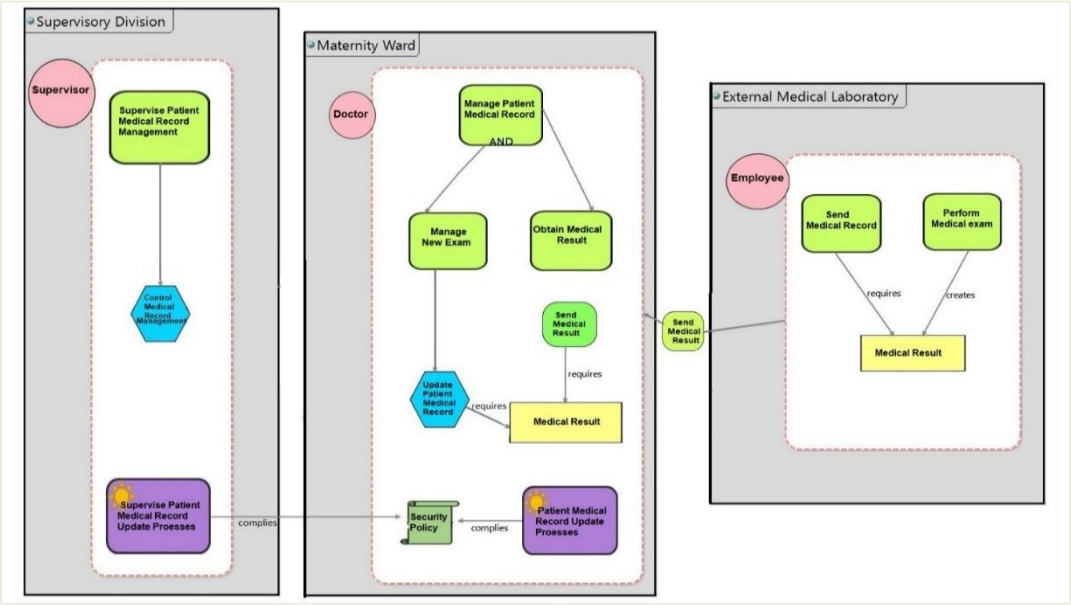

Fig 4: Organization View of Managing Patient Records (Alkubaisy et al., 2021)

the patient's record conflicts with the accountability principles as the accountability requires validation of the data. Considering the following scenario: Patient's medical record is met with a conflict for anonymity. Validation of Medical examination is met with the conflict for accountability. Sending Medical results is met with the conflict for confidentiality and integrity.

Phase 2: Identify Conflicts between Requirements and Conflict Decisions

We have divided a few key terms to help you figure out which ones are in conflict between security and privacy as presented in Table 2. For instance, Authentication and Undetectability are in conflict. Another example is of a conflict between Anonymity and Availability. According to the motivation scenario in terms of security and privacy requirements, assume a patient's doctor has ordered some medical test. A lab test was required for the patient. As a result, the lab will send the doctor's report with the patient's results; by maintaining the report's integrity and confidentiality. Next, the doctor will update patient's record according to GDPR's accountability principles. Privacy by design principles recommend anonymity to be top priority for updating a patient's medical record while results should be approved by a senior supervisor, and therefore accountability is a must in this case. Therefore, there is conflicts between accountability as security requirement and anonymity as privacy requirement. While the patient's record must be updated anonymously but there should also be an accountability record to cross-check drug recommendation when an audit is conducted or there is a need for an investigation for Doctor's misconduct. Many cases, like the one involving the doctor, patient, and lab examiner, have more than one requirement. Thus, it must follow both security and privacy principles, which is a difficult decision, and thus a major conflict arises. The case of anonymity and accountability is significant because the former allows users to use resources or make decisions without revealing their identity while the latter contradicts and relates each action to a participant. To conclude, Phase 2 discussed identification of the conflict between a Doctor and his Supervisor in terms of accountability and anonymity.

Phase 3: Conflict Resolution Patterns

In Phase 3 we discuss Conflict Mitigation by addressing the requirements to be followed, and then presenting possible solutions for mitigating the conflict. In order to mitigate the conflict with the help of a supporting tool, each conflict case must first define the problem and identify the restrictions that must be followed. This supporting tool will be added to a Privacy Pattern Library and will be applied in a scenario in SecTro. It will provide to requirements of both sides and will relate to each individual conflict to produce feasible solutions as depicted in Figure 5. First, requirements analyst must identify measures related to security and privacy concerns to support and improve constraints. Then, related to support and execution of the established route of plan by following mechanisms identified in security and privacy domains. According to [7] alongside identifying measures with the help of experts, a security and privacy catalogue is recommended to be used if need arises in such complex situations. A Design Pattern Library (DPL) is formulated and added in SecTro2. Various experts develop models according to the identified conflict and can save it for later use. These models as available on DPL are then accessed by the Developer to resolve security and privacy conflicts.

In this case we were able to identify two supporting tools, titled: IDEMIX and Cryptography Supporting Tool. Cryptography couldn't address the anonymity concern even though it was suitable for maintaining confidentiality and integrity. IDEMIX was established as the more suitable one because it adheres to GDPR's Data minimization principle by making the medium of file sharing anonymous [27] between users and service provider, this resolving the conflict between the Doctor and his supervisor while also maintaining the accountability perspective. In addition, we added supporting tools in Privacy by Design View in figure 5 in which we can add new concepts/ tools to import a suitable mechanism according to the conflict identified. Additionally, DBL also supports Data Record Action along with IDEMIX were identified as supporting tools in DBL.

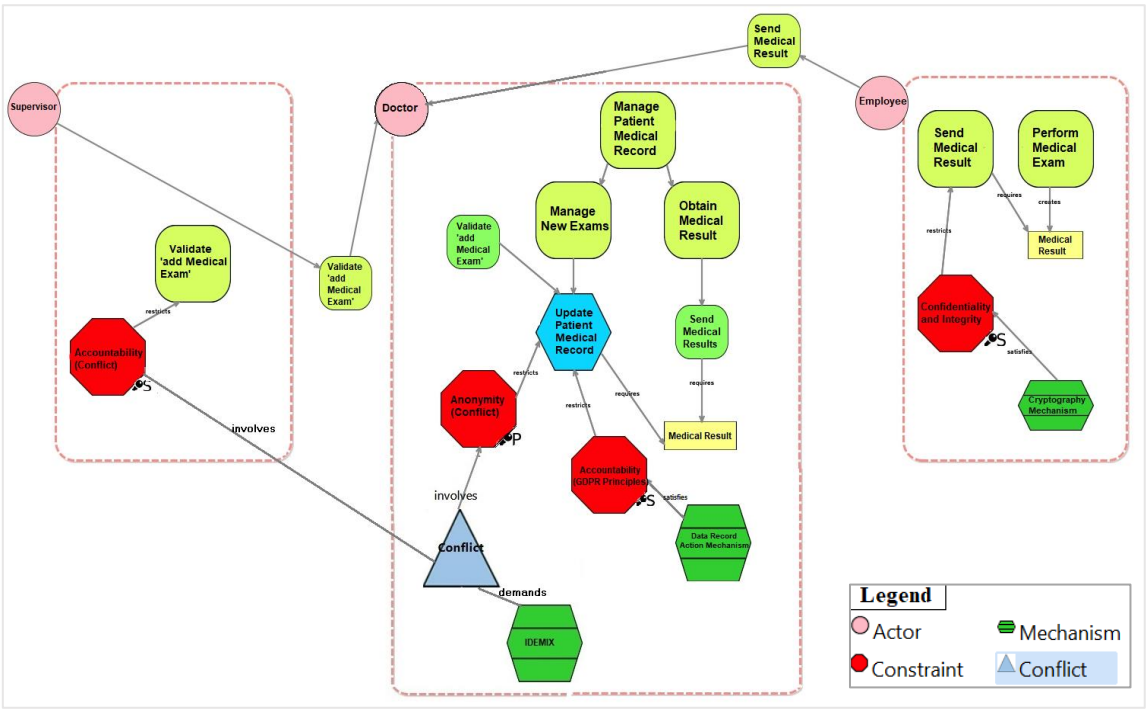

Fig 5. Integrating conflict resolution in Privacy-by-Design view of Managing Patient Records (Alkubaisy et al., 2021)

Discussion

For the entire process of updating the Patient Medical Record, there is a strong need to deal with the anonymity concern. The anonymity of the doctor is important so that no one knows who made the change on the records. This concern is fulfilled through a mechanism. IDEMIX is there to cater to this concern. For the accountability requirement, the supervisor needs to authorize the change. This is where the conflict lies because anonymity is compromised in this case. There is a conflict between anonymity and accountability. This problem can be resolved by the IDEMIX mechanism [24]. This will ensure minimized release of personal information hence keeping the anonymity intact. IDEMIX is an optimizing cryptographic compiler that provides a great level of assurance. This keeps the transport medium between the users and service providers anonymous. This technique ensures anonymity, authenticity, and accountability of transactions between the users and service providers. Furthermore, the requirements of integrity and anonymity are also fulfilled by cryptographic mechanisms while sending medical records. Lastly, the concern of accountability is catered through the Record Data Action mechanism. Using these combinations of mechanisms and techniques we can meet all the requirements

and resolve all the conflicts that may arise in this process. These mechanisms help us achieve anonymity, integrity, and accountability in the whole process.

6. Evaluation

6.1 Evaluation Strategy

We employ qualitative and quantitative analyses to achieve a comprehensive evaluation. For the qualitative aspect, we designed a focus group session, with participants who are experts in software engineering and researchers. Before we undertook the evaluation, we constructed a pilot focus group evaluation with three participant groups − PhD student, PhD doctor and Research Fellow. This revealed to us the possibilities of improving the focus group evaluation according to the participants' feedback. Moving forward, we could perform the full-scale focus group evaluation of fifteen participants. The fifteen participants were active researchers in the fields of software engineering and were practicing at different universities across various countries to add multi-dimensional and multi-perspective value to our heterogeneous approach.
Qualitative and quantitative analysis are critical parts of the evaluation strategy. Based on qualitative and quantitative analysis, each complete evaluation is scaled. Both aspects are approached in different methods by the researchers. The objective is to establish a critique of the frameworks and highlight the flaws which can be fixed for improvements. A pilot focus group has to be created before the evaluation begins.

According to the policy for ethical research in the United Kingdom, parts of the research methods and data of a research study are subject to ethical review because of the involvement of human participants. Ethical review self-assessment forms and a data management plan were submitted to the Ethics and Integrity Officer of the University. The ethical review forms included details of the project and self-assessment questions.

6.2 Full Evaluation

To design the evaluation of the framework, we have mentioned that some of the steps of ConfIS framework are semi-automated, while others are manual

steps, based on the analyst's point of view. First, the conflicts between requirements are identified, based on a matrix presented by a previous study [3] Hence, we sort the requirements that could lead to a potential conflict. After identifying the requirements which are in conflict, the analyst must decide whether this kind of conflict would affect the system, based on the presented scenarios. Therefore, the first phase of the framework is performed manually by the software requirements analyst. Phase 2 identifies the potential conflicts between requirements that were detected in the previous phase. The final phase proposes conflict resolution patterns by matching the problem to a resolution pattern for each conflict that the analyst might face. These patterns act as a reference for the analyst to resolve conflicts between requirements. The final phase of our framework is automated by using SecTro tool (by importing a privacy pattern library)

6.3 Results

A summary analysis of the evaluation survey reveals that the majority of respondents were research fellows (47%), followed by PhD students (33%) and doctor (20%). All participants found the research design questions were appropriate, useful, well presented (87%) and the research field quite interesting (93%) in gaining their feedback. On the other hand, just 54% agreed that the results were clearly presented; this leaves room for improvement (Figure 5).

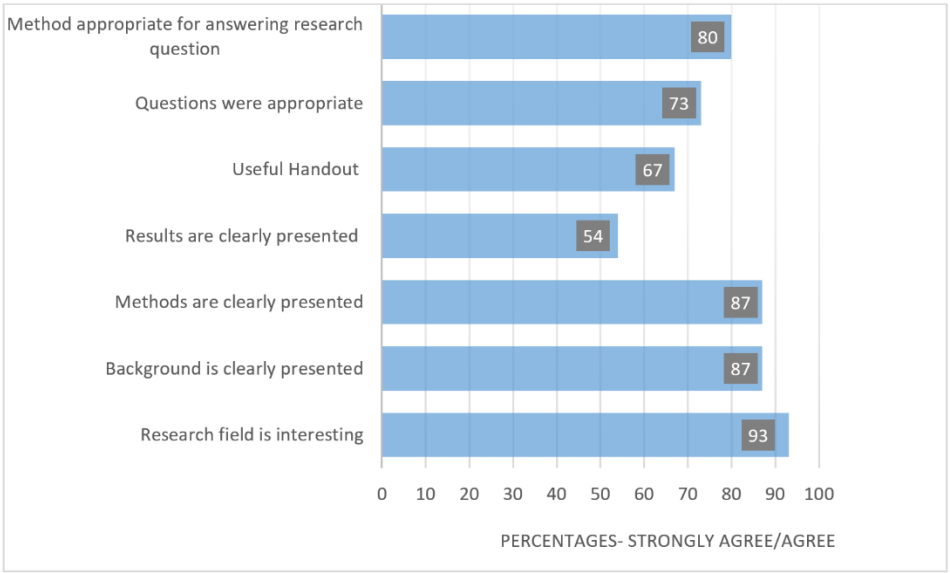

Fig 5. Research Design

More than 80% of the research fellows who participated highly agreed with the research design saying that the research field is interesting, background and methods are clearly presented and appropriate for answering the research questions, the handout is useful, and questions are appropriate. Furthermore, 100% of the PhD doctors who participated highly agreed that the research field is interesting, and that the background is clearly presented. Moreover, over 60% (the majority) did agree to the method being clearly presented and appropriate for answering the research questions. A neutral response was provided, however, to whether the results were clearly presented, the usefulness of the handout and appropriateness of questions. Additionally, most PhD students, over 60%, agreed with the research design, Figure above. In instances of participants disagreeing with it to some degree. Additionally, the general framework was well received by the majority, proving to be sequentially in order (87%), clear and well defined (80%), easy to analyze (80%) and for making feasible decisions such as reducing cost, conflict, and faster development processing (73%) (Figure 6).

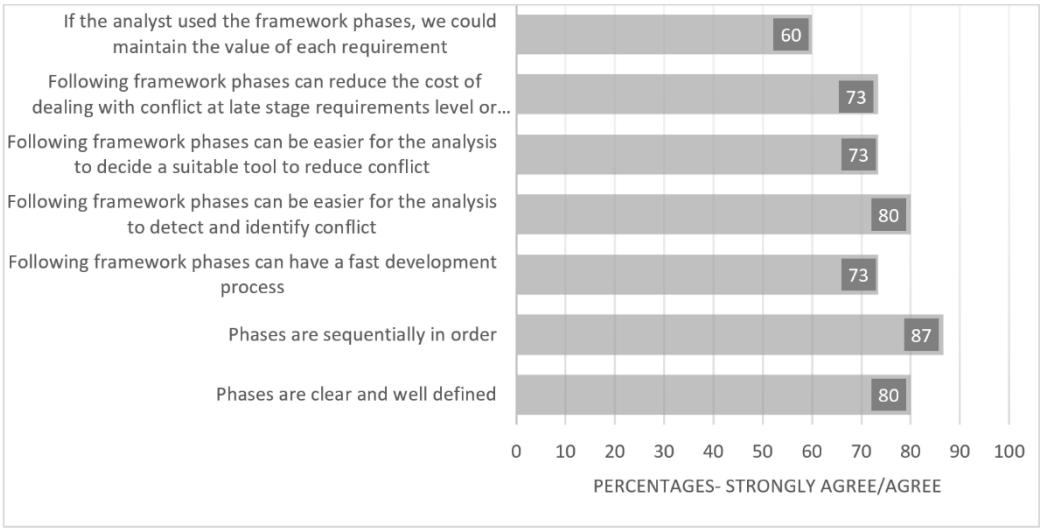

Fig 6. General Framework (Alkubaisy et al., 2021)

The majority share, well over 70% of research fellows, agreed with the general framework. They approve of the statements that the relevant phases are clear, well defined, sequentially in order, can have a fast development process, are easy for identifying conflict, reducing it and its relevant costs, and maintaining

the value of each requirement. Additionally, more than 80% of PhD students agreed with the design of the general framework and its phases. Phase 1, mapping security and privacy requirements, showed 70-87% of participants agreeing to the presentation of Phase 1 while Phase 2 was well received with the majority (80-86%) agreeing that the researcher adequately addressed conflicts between requirements and decisions. Additionally, feedback on Phase 3 showed varying responses (67-87%), yet the participants still agreed that there was an ease to understanding conflict resolutions patterns and its supporting tools (Table 3).

Table 3. ConfIS Framework Phases and Survey Responses

Phase 1: Mapping Security and Privacy Requirements	70-87% (strongly/agree)
Phase 2: Identify Conflicts between Requirements and Conflict Decisions	80-86% (strongly/agree)
Phase 3: Conflict Resolution Patterns	67-87% (strongly/agree)

Analysis of ConfIS Framework Phases' Focus Group Results and Survey Responses

Ven & Delbecq [25] found that a two-stage combination of focus group and the nominal group technique (NGT), coined as 'nominal focus group', was particularly effective as an evaluation method. The nominal group process is a structured meeting which seeks to provide an orderly procedure for obtaining qualitative information from target groups who are most closely associated with a particular issue. It allows the meetings' participants to determine which issues require further, more in-depth inquiry and to draw attention to issues that may have been previously unidentified. This evaluation method is used in this research to rank in order of importance the participants' responses to Phases 1 and 2. In order of importance for Phase 1, the top three security requirements are seen to be integrity, confidentiality, and accountability, while anonymity, unobservability and pseudonymity are ranked top highest in privacy requirements. Participants' responses to identifying possible conflicts between requirements as depicted in Phase 2, show accountability and anonymity mostly chosen, followed by auditability and anonymity and accountability and undetectability. Anonymity accounts for a large percentage of Phase 2 (Figure 7).

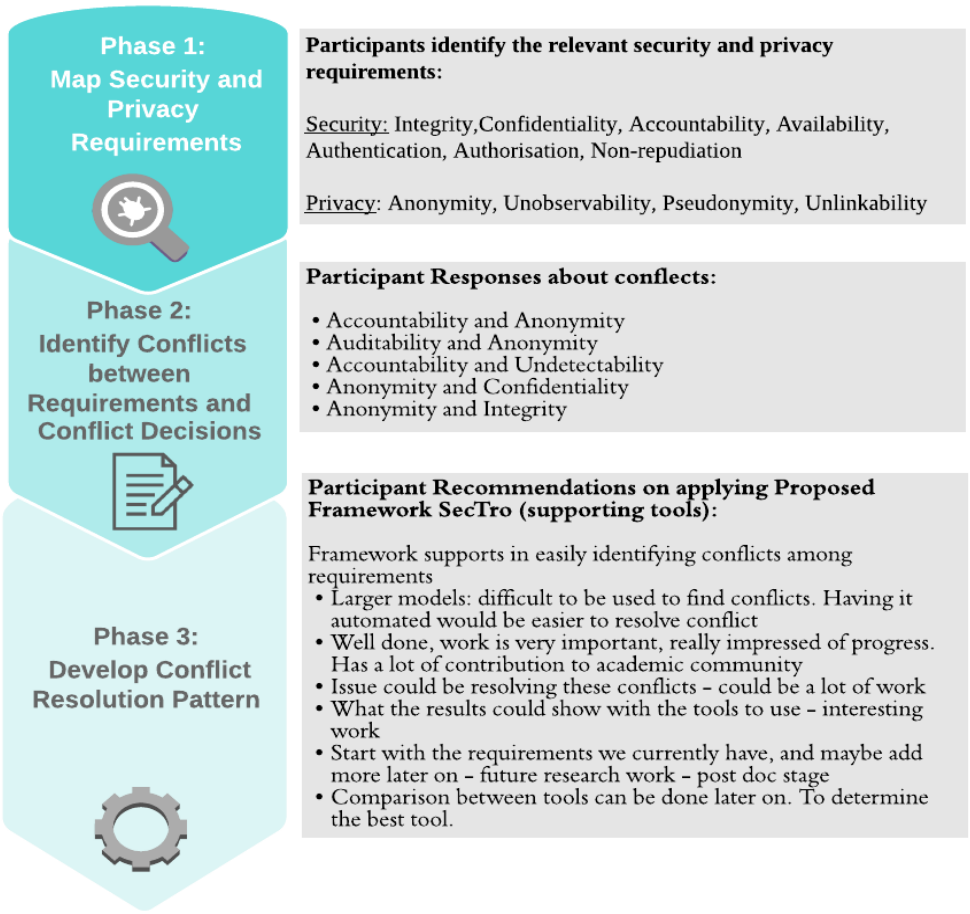

Fig 7. ConfIS Framework and Focus Group Response using Nominal Ranking Evaluation Method

7. Application to ConfIS Framework

In pursuit of answering **RQ1**: How to design a framework supporting the analyst to identify and resolve conflicts between privacy and security requirements? A list of Security and Privacy Requirements, supported by the literature review we conducted, has been developed as a part of **Phase 1: Mapping Security and Privacy Requirements**. This list is presented in Table 1. Additionally, **RQ1** is also supported by the mapping matrix we stipulated in **Phase 1:**

Mapping Conflicts between security and privacy requirements. **RQ1** addressed by employing SecTro as mentioned earlier. SecTro creates models of the requirements for information systems [17]. By extending SecTro to our proposes framework, we offer the analyst a way forward to identify and resolve conflicts using a mapping matrix presented in Table 2. The framework is then validated according to the DEFeND project's stipulations [18], ensuring compliance with GDPR in the process. Moreover, we aim to answer **RQ2**: How to support the analyst in the identification and resolution of conflicts between requirements in a systematic and tool-supported way in real cases? In **Phase 2: Identify Conflicts between Requirements and Conflict Decisions**, we provide the analyst with the necessary and pertinent tools. It is seen that our proposed framework also seeks to mitigate conflicts, under the condition that both the Phases 1 and 2 are adequately fulfilled. Lastly, with **Phase 3: Conflict Resolution Patterns**, including its table and design view, we provide an approach to mitigating conflicts.

8. Related Work

Many types of research have been conducted in this field of study. Many researchers have come up with their theories and worked hard on constructing mechanisms to deal with conflicts and find their solutions. Professionals with knowledge in requirements elicitation methodologies, based on systematic procedures and methods, are required, according to a recent study [26], to enhance software requirements with crucial security and privacy aspects.

Ramadan *et al.* conducted several studies in this field of study [27, 28]. Their data showed how conflicts can be detected between data-minimization and security requirements. This was investigated in business process models and conflicts between security and privacy requirements in a system were examined. Salnitri and fellow researchers had conducted a study related to this same subject in 2020 [29]. They had come up with an innovative method which was called SePTA (Security, Privacy and Trust Approach). As the name suggests, this procedure supported all three aspects which are security, privacy, and trust. These requirements were supported under only one framework. This framework was majorly designed for sociotechnical systems because this helped software designers and security experts to satisfy these requirements. In terms of dealing with such conflicts involving goals and/or requirements, we introduced risk based on the user concern, trustworthiness goals, and requirements as determinants to TrustSoFt in our previous work.

In the work of Horkoff, 246 top-cited papers were examined in the span of 20 years [30]. They have focused their study on the Goal-oriented requirements engineering (GORE) area. In this field, goals are used as the main subject. Goals are utilized and used as a baseline to elicit, model, and analyze requirements. A survey paper compared recent studies in this field [31]. This talked about the conflict between requirements in the early stage of development. The survey consisted of various case studies regarding software engineering under the requirement gathering techniques. It further talked about how conflicts could be resolved at the early phase. Regarding resolving the conflicts, usage of the agile software development method was also elaborated. Maxwell *et al.* also includes the identification of conflicting software requirements [32]. They highlighted the rules and laws which made them easier to handle. They further mentioned that the reputation of a company highly depends on the rules and ethics that they follow, which increases the importance of these rules. We can't ignore the extra costs that these laws and regulations might bring. According to their perspective of Schon *et al.* [33], agile software development made the changing of requirements easy and fast which further made it simple to handle. But with the rapidness it provided, more complexities were also created because a hybrid development model was used in this.

It is important to mention that privacy became an important aspect at this time, as we mentioned in introduction section. As we find out that there are more that regulation and laws concern privacy disclosure. For instance, Brazilian citizens' complaints regarding data privacy are rising by the day, particularly with the access into force of the General Data Protection Law (LGPD) [34]. The purpose of the Act is to regulate the handling of personal data. If personal data processing is not done in compliance with this regulation, it might have a lot of consequences in technical fields. LGPD is a piece of legislation that gives Brazilian citizens privacy, allowing them to identify and amend data processing at any anytime. Organizations that apply the LGPD will demonstrate their integrity and dedication to their users. Therefore, LGPD provides numerous principles that will help both citizens and organizations, in addition to showing how risk management has improved and organizational techniques have improved. Some aspects may have affected organizations' LGPD requirement specification in the Brazilian environment. Moreover, The California Consumer Privacy Act (CCPA) [35], a digital privacy regulation that offers consumers more control over their online personal information, was approved by California lawmakers in 2018. In the United States, the CCPA is a major rule that regulates how technology firms acquire and use data. (CCPA) recognizes various categories of personal information. The CCPA, on either hand, exempts public

access information, which is described as "information lawfully made available from federal, state, or provincial government records, but not if the aim of data processing is incompatible with its declared purpose." Regulations may be required for such organisations to comply. Additionally, it is in companies' best interests to establish compliance strategies beforehand and rather than be caught unawares by last-minute implementation or significant complaints.

9. Conclusion

The nature of software development for realistic systems presents a complex phenomenon of conflict resolution. Usually in engineering software systems, the conflict arises between security and privacy. This article presented a three -phases framework, called ConfIS, to identify conflicts between security and privacy requirements and to find solutions that could mitigate these conflicts. This framework allows the analyst to look at the potential conflicts beforehand that may arise in the future. ConfIS has been applied to a case study from the DEFeND project. A step-by-step demonstration of the phases of ConfIS has been presented. We plan to add CCPA and LGPD support to the ConfIS framework in the future. Using different case studies that are in accordance with the regulations.

10. Acknowledgement

This work has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 787068.

References

1. Alkubaisy, D., Piras, L., Al-Obeidallah, M.G., Cox, K.,Mouratidis, H.: ConfIs: A Tool for Privacy and Security Analysis and Conflict Resolution for Supporting GDPR Compliance through Privacy-by-Design. In: 16th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE) (2021)
2. Alkubaisy, D.: 'A framework managing conflicts between security and privacy requirements', 2017 11th international conference on Research Challenges in Information Science (RCIS), Institute of Electrical and Electronics Engineers, pp. 427–432. doi: 10.1109/RCIS.2017.7956571. (2017).
3. Alkubaisy, D., Cox, K. & Mouratidis, H.: 'Towards detecting and mitigating conflicts for privacy and security requirements,' in Kolp, M. et al. (eds.) Proceedings: RCIS 2019 - IEEE 13th international conference on Research Challenges in Information Science: Towards a design science

for information systems. Brussels, 29–31 May 2019, Belgium: Institute of Electrical and Electronics Engineers Computer Society. Available at: https://doi.org/10.1109/RCIS.2019.8876999 (Accessed 05 Dec 2020) (2019).

4. Noll, Thomas. "Safety, dependability and performance analysis of aerospace systems." International Workshop on Formal Techniques for Safety-Critical Systems. Springer, Cham, 2014.
5. Tejas, R. Shah, and S. V. Patel. "Security, privacy and trust oriented requirements modeling for examination system." 2012 Nirma University International Conference on Engineering (NUiCONE). IEEE, 2012.
6. Dubois, Eric, and Haralambos Mouratidis. "Guest editorial: security requirements engineering: past, present and future." (2010): 1-5.
7. Mouratidis, H. et al. 'A framework to support selection of cloud providers based on security and privacy requirements'. Journal of Systems and Software, 86(9), pp. 2276–2293 (2013).
8. Albrecht, Jan Philipp. "How the GDPR will change the world." Eur. Data Prot. L. Rev. 2 (2016): 287.
9. Kim, M., Park, S., Sugumaran, V., Yang, H., Managing requirements conflicts in software product lines: A goal and scenario-based approach, Data Knowl. Eng., vol. 61, no. 3, pp. 417-432, Jun. (2007).
10. Egyed, A. & Boehm, B. 'A comparison study in software requirements negotiation', Proceedings of the 8th annual international symposium on systems engineering, INCOSE'98, (1998).
11. Lamsweerde, A., Darimont, R. & Letier, E. 'Managing conflicts in goal-driven requirements engineering', IEEE Transactions on Software Engineering, (24)11, pp. 908–926 (1998).
12. Schär, B. Requirements engineering process: HERMES 5 and SCRUM. Master's Thesis. University of Applied Sciences and Arts (2015).
13. Botha, Johnny, Marthie Grobler, and Mariki Eloff. "Global data breaches responsible for the disclosure of personal information: 2015 & 2016." European Conference on Cyber Warfare and Security. Academic Conferences International Limited, 2017.
14. Aldekhail, M., Azzedine, C. & Djamal, Z. 'Software Requirements Conflict Identification: Review and Recommendations,' International Journal of Advanced Computer Science & Applications, 7(10), pp. 326–335 (2016).
15. Mairiza, D., Zowghi, D. & Gervasi, V. 'Conflict characterization and analysis of non functional requirements: An experimental approach', IEEE 12th International conference on intelligent software methodologies, tools and techniques (SoMeT) Budapest: Institute of Electrical and Electronics Engineers, pp. 83–91 (2013).
16. Pavlidis, M. & Islam, S. 'SecTro: A CASE tool for modelling security in requirements engineering using secure Tropos'. CEUR Workshop Proceedings, 734, pp. 89–96 (2011).
17. Mouratidis, Haralambos. "Secure software systems engineering: the secure tropos approach." J. Softw. 6.3 (2011): 331-339.
18. Piras, L. et al. 'DEFeND architecture: A privacy by design platform for GDPR compliance', in Gritzalis S. et al. (eds.) Trust, privacy and security in digital business. Proceedings of 16th international conference, TrustBus 2019. Cham, Switzerland: Springer, pp. 78–93 (2019).
19. Yahuza, M. et al. 'Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities', Institute of Electrical and Electronics Engineers Access, 8, pp. 76541–76567 (2020).
20. Mouratidis, H. & Giorgini, P. 'Secure Tropos: A security-oriented extension of the Tropos methodology'. International Journal of Software Engineering and Knowledge Engineering, 17(02), pp. 285–309. Available at:

http://www.worldscientific.com/doi/abs/10.1142/S0218194007003240 (Accessed: 10 February 2016) (2007).

21. Salado, A. & Nilchiani, R. 'The concept of order of conflict in requirements engineering'. Institute of Electrical and Electronics Engineers Systems Journal, 10(1), pp. 25–35 (2014).
22. Piras, L. et al. 'DEFeND DSM: A data scope management service for model-based privacy by design GDPR compliance', in Gritzalis S. et al. (eds.) Trust, privacy and security in digital business. Lecture Notes in Computer Science, vol 11711. Cham, Switzerland: Springer, pp. 186–201 (2020).
23. Piras, Luca, et al. "A DATA SCOPE MANAGEMENT SERVICE TO SUPPORT PRIVACY BY DESIGN AND GDPR COMPLIANCEa." Journal of Data Intelligence 2.2 (2021): 136-165.
24. Camenisch, J. & van Herreweghen, E. 'Design and implementation of the idemix anonymous credential system', Proceedings of the 9th ACM cofnference on Computer and communications security. New York, NY: Association for Computing Machinery, pp. 21–30. doi:https://doi.org/10.1145/586110.586114 (2002).
25. Ven, A. H. van de and A. Delbecq. "The nominal group as a research instrument for exploratory health studies." American journal of public health 62 3: 337-42 (1972).
26. Mendes, L. M., de Franco Rosa, F., & Bonacin, R. (2021). Enriching Financial Software Requirements Concerning Privacy and Security Aspects: A Semiotics Based Approach. In ITNG 2021 18th International Conference on Information Technology-New Generations (pp. 85-90). Springer, Cham.
27. Ramadan, Q. et al. 'Detecting conflicts between data-minimization and security requirements in business process models, in Pierantonio, A. & Trujillo, S. (eds.) European Conference on Modelling Foundations and Applications. Lecture Notes in Computer Science, vol 10890. Cham, Switzerland: Springer, pp. 179–198 (2018).
28. Ramadan, Q. et al. 'A semi-automated BPMN-based framework for detecting conflicts between security, data-minimization and fairness requirements'. Software and Systems Modeling, 19, pp.1191–1227. doi:10.1007/s10270-020-00781-x 2020).
29. Salnitri, M. et al. 'Modelling the interplay of security, privacy and trust in sociotechnical systems: A computer-aided design approach'. Software and Systems Modeling, 19(2), pp. 467–491 (2020).
30. Horkoff, J. et al. 'Goal-oriented requirements engineering: an extended systematic mapping study,' Requirements Engineering, 24(2), pp. 133–160 (2019).
31. Bhavsar, R. et al. 'Resolving conflicts in requirement engineering through agile software development: A comparative case study', in Bhattacharyya, S. et al. (eds.) International Conference on Innovative Computing and Communications. Singapore: Springer, pp. 349–357 (2019).
32. Maxwell J. C., Antón, A. I. & Swire, P. 'A legal cross-references taxonomy for identifying conflicting 160 software requirements', 2011 IEEE 19th international requirements engineering conference, 161, pp. 197–206 (2011).
33. Schon, E. -M., Thomaschewski, J. & Escalona, M. J. 'Agile requirements engineering: A systematic literature review'. Computer Standards and Interfaces, 49, pp. 79–91 (2017).
34. Ferrão, S. É. R., Carvalho, A. P., Canedo, E. D., Mota, A. P. B., Costa, P. H. T., & Cerqueira, A. J. (2021). Diagnostic of Data Processing by Brazilian Organizations—A Low Compliance Issue. Information, 12(4), 168.
35. Mulgund, Pavankumar, et al. "The implications of the California Consumer Privacy Act (CCPA) on healthcare organizations: Lessons learned from early compliance experiences." Health Policy and Technology 10.3 (2021): 100543.