Information and Software Technology 56 (2014) 273–293

Contents lists available at ScienceDirect

Information and Software Technology

journal homepage: www.elsevier.com/locate/infsof

A systematic review on security in Process-Aware Information Systems – Constitution, challenges, and future directions ☆

Maria Leitner *, Stefanie Rinderle-Ma

University of Vienna, Faculty of Computer Science, Research Group Workflow Systems and Technology, Waehringerstrasse 29, 1090 Vienna, Austria

ARTICLE INFO

Article history:
Received 28 January 2013
Received in revised form 21 November 2013
Accepted 5 December 2013
Available online 16 December 2013

Keywords:
Business Process Management
Business process security
Process-Aware Information Systems
Security
Systematic literature review
Workflow security

ABSTRACT

Context: Security in Process-Aware Information Systems (PAIS) has gained increased attention in current research and practice. However, a common understanding and agreement on security is still missing. In addition, the proliferation of literature makes it cumbersome to overlook and determine state of the art and further to identify research challenges and gaps. In summary, a comprehensive and systematic overview of state of the art in research and practice in the area of security in PAIS is missing.
Objective: This paper investigates research on security in PAIS and aims at establishing a common understanding of terminology in this context. Further it investigates which security controls are currently applied in PAIS.
Method: A systematic literature review is conducted in order to classify and define security and security controls in PAIS. From initially 424 papers, we selected in total 275 publications that related to security and PAIS between 1993 and 2012. Furthermore, we analyzed and categorized the papers using a systematic mapping approach which resulted into 5 categories and 12 security controls.
Results: In literature, security in PAIS often centers on specific (security) aspects such as security policies, security requirements, authorization and access control mechanisms, or inter-organizational scenarios. In addition, we identified 12 security controls in the area of security concepts, authorization and access control, applications, verification, and failure handling in PAIS. Based on the results, open research challenges and gaps are identified and discussed with respect to possible solutions.
Conclusion: This survey provides a comprehensive review of current security practice in PAIS and shows that security in PAIS is a challenging interdisciplinary research field that assembles research methods and principles from security and PAIS. We show that state of the art provides a rich set of methods such as access control models but still several open research challenges remain.

Contents

1. Introduction . . . 274
   1.1. Process-Aware Information Systems and Security . . . 274
   1.2. State of the art . . . 274
   1.3. Contribution . . . 275
2. Research methodology . . . 275
   2.1. Research identification . . . 275
   2.2. Literature search . . . 275
   2.3. Literature selection . . . 276
   2.4. Data extraction and synthesis . . . 276
   2.5. Classification of security controls . . . 277
3. Results . . . 278
   3.1. Overview of selected publications . . . 278
      3.1.1. Publication years . . . 278

* Corresponding author. Tel.: +43 1 4277 79124; fax: +43 1 4277 8 79124.
E-mail addresses: maria.leitner@univie.ac.at (M. Leitner), stefanie.rinderle-ma@univie.ac.at (S. Rinderle-Ma).

0950-5849/$ - see front matter © 2013 The Authors. Published by Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.infsof.2013.12.004

3.1.2. Publication sources . . . 278
3.2. Security in Process-Aware Information Systems . . . 278
3.3. Security controls . . . 280
3.3.1. Security concepts . . . 281
3.3.2. Authorization and access control . . . 281
3.3.3. Verification . . . 283
3.3.4. Failure handling . . . 284
3.3.5. Applications . . . 285
4. Classification of security controls . . . 286
Q3.1: Is security enforced in every phase of the process life cycle? . . . 286
Q3.2: Which types of security controls are utilized in PAIS? . . . 287
5. Research challenges . . . 287
6. Discussion . . . 288
6.1. Main findings . . . 288
6.2. Impact on research and practice . . . 288
6.3. Limitations of this review . . . 289
7. Conclusion . . . 289
Appendix A. Supplementary material . . . 289
References . . . 289

1. Introduction

The adequate support of business processes constitutes a crucial challenge for enterprises through all application domains. Hence, Business Process Management (BPM) and the support of Process-Aware Information Systems (PAIS) has become a major research area nowadays.

1.1. Process-Aware Information Systems and Security

Process-Aware Information Systems (PAIS) support the automated enactment and execution of business processes [1]. Often, these systems involve a multitude of participants and manage large data sets. Imagine, for example, a hospital with hundreds of employees managing the (information) flow of daily processes such as patient admission, examination, release, or surgeries. Such processes involve many participants (e.g., doctors, patients, and administrative staff), employ resources (e.g., X-ray machines and databases) and manage public and private information (e.g., patient records, lab results, and medical images). Furthermore, process choreographies and inter-organizational business processes fulfill business operations over one or more domains. Often, these processes are enacted over the web or in a cloud. In these infrastructures, security can be an issue (cf. [2]).

It is a PAIS characteristics to offer support for task automation as well as for human interaction. Both aspects are of importance when it comes to security. Reasoning about automatic processes and their correctness in regard to certain requirements is as crucial as to consider security from a human perspective. Examples for the latter are as attackers with malicious actions or insiders with unintentional, security threatening actions.

The level of abstraction a PAIS application exhibits can be characterized by using an enterprise architecture model (e.g., [3,4]). This paper provides a extensive literature review that investigates security controls across all layers, as security architectures are an example for cross-layer views (cf. [3]).

Furthermore, most enterprises and organizations have to fulfill legal requirements. For example, the Health Insurance Portability and Accountability Act (HIPAA) §1173(d)(2)(AB) states that each person who maintains or transmits health information has to *(A) ensure the integrity and confidentiality of the information; (B) to protect against any reasonably anticipated (i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information*. This federal law does not only affect hospitals but also anyone who handles health information e.g., general practitioners, specialists, medical labs, and paramedics. In fact, many of these legal or regulatory restrictions refer to legal requirements to enforce security (e.g., to prevent unauthorized access) and can be found in regulations and law worldwide such as U.S. Code (U.S.C.) 44 Section 3542 (2012) or EU Directive 95/46/EC of 24 October 1995. Adherence to legal requirements, employment of different process participants, handling possibly sensitive data, and distributed process scenarios are only some of the reasons that require security to become a key concern in PAIS.

1.2. State of the art

Although research has started to investigate the topic of security in PAIS, current state of research and practice on security in PAIS is unbalanced. First of all, an agreement on a common terminology or requirements on security in PAIS as well as widely accepted guidelines or models are missing, although, there is a general understanding that security in PAIS is a key challenge. One reason could be that since the proposition of security considerations by the Workflow Management Coalition (WfMC) as global organization for process related standards in 1998 [5], the maturing of the PAIS research as a discipline [6] has not been accompanied with further standardization efforts and developments with respect to security. Another reason is that PAIS research has centered on the design and development of core PAIS-relevant features when addressing security-related questions so far. In fact, security in PAIS should constitute a rather interdisciplinary research field, bringing together different disciplines such as PAIS/BPM and security (in particular, information security). This provides new challenges such as defining security in PAIS or applying methods from both disciplines. Finally, certain process scenarios such as processes that are executed in a collaborative manner among different partners have not been considered with respect to security, although such scenarios pose high demands on security and confidentiality (e.g., a partner should not be able to access details of the other partner's process). Altogether, a review of terminology and concepts as currently used in PAIS security, the analysis of questions and existing approaches addressing PAIS security as an interdisciplinary research area, and the investigation of challenges and existing solutions for security in advanced process scenarios could significantly contribute to a common and deeper understanding within the PAIS discipline, but also within the different related disciplines such as information security.

1.3. Contribution

This paper provides a systematic literature review [7,8] on security in PAIS targeting the following research questions:

(1) What does security in Process-Aware Information Systems mean (terminology, common understanding, particularly addressing the interfaces with related areas)?
(2) Which security controls are currently utilized in Process-Aware Information Systems?
(3) Is security enforced in every phase of the process life cycle?
(4) What are the challenges of current security research in Process-Aware Information Systems?

Section 2 outlines the different steps of the literature review starting from research identification (see questions above), literature search (resulting in a total of 424 papers), literature selection (resulting in a set of 275 finally relevant papers), data extraction and synthesis, and the classification of security controls. Based on the literature review, we identify existing definitions and terminology for security in PAIS (cf. Section 3.2). This includes a discussion of security in PAIS as an interdisciplineray research area. As another result of the literature review, Section 3.3 introduces currently applied security controls in PAIS that can be clustered into five categories. In order to identify open research questions and challenges, the identified security controls are classified along the two dimensions *process life cycle phase* and *action type* in Section 4. Process life cycle phase refers to the time when a certain security control is applied according to existing approaches, for example, during the design or execution phase of a process. Action type describes whether a security control is regarded as preventive, detective, or reactive. The resulting research challenges are discussed in Section 5. In Section 6, we summarize the main findings of the paper and elaborate on their potential impact on research and practice. Further on, this section discusses limitations of the conducted literature review. Section 7 concludes the paper.

2. Research methodology

In this survey, a systematic literature review [7,8] is carried out based on guidelines for research synthesis (e.g., [9]). The research methodology of this paper is outlined in Fig. 1. First, research questions are defined. Then, an extensive literature search is conducted and further literature is selected. Based on the resulting data set, we synthesize the literature in categories and security controls. Additionally, we classify these controls to identify research challenges.

2.1. Research identification

The goal of this paper is to examine and evaluate security research in Process-Aware Information Systems (PAIS). We approach this aim by answering the following research questions (Q) refining the questions formulated in Section 1.

Q1. What does security in Process-Aware Information Systems mean (terminology, common understanding, particularly addressing the interfaces with related areas)?
Q2. Which security controls are currently utilized in Process-Aware Information Systems?
Q3. What are the challenges of current security research in Process-Aware Information Systems?
  Q3.1 Is security enforced in every phase of the process life cycle?
  Q3.2 Which types of security controls are utilized in Process-Aware Information Systems?

The first question (Q1) investigates how research specifies security in PAIS and which methods are currently used to provide security in PAIS. Q1 aims at identifying relevant related work i.e., defining keywords for the literature search that lead to a maximum coverage of related approaches. We noticed that the terms *"workflow security"* or *"business process security"* are not commonly used to identify security-related literature. In fact, other keywords such as authorization or access control are mostly used. Hence, we additionally searched within the references of the retrieved literature and manually checked with researchers having expertise in security in PAIS to verify that all topic-relevant research is examined. From the retrieved literature we synthesize the data to identify the main categories and security controls in PAIS (Q2). Classifying approaches along the process life cycle consisting of the phases design, enactment and execution, evaluation, and change has proven to be a viable method to gain a holistic view [1]. Therefore, question Q3.1 examines security research in PAIS along the process life cycle. Based on the results of questions (Q3.1) and (Q3.2), the last question (Q3) aims at investigating research challenges and gaps.

2.2. Literature search

A manual search was conducted including horizontal and vertical searches. Google Scholar (http://scholar.google.com) and the free search of DBLP (http://dblp.isearch-it-solutions.net/dblp/) were used to perform horizontal (general) searches. In addition, the libraries of the computer science publishers IEEE Computer Society (http://www.computer.org/), ACM (http://dl.acm.org/), and Springer (http://www.springerlink.com/) were searched. The keywords *"workflow security"* and *"business process security"* were used in all searches (retrieving dates: 02/01/2011 and 10/01/2012). In case of vertical searches, relevant journals (Information Systems, Data & Knowledge Engineering, MIS Quarterly, Transactions on Information and System Security (TISSEC), Computers & Security, Journal of Computer Security) and conference proceedings (Business Process Management (BPM), Cooperative Information Systems (CoopIS), Conference on Advanced Information Systems Engineering (CAiSE), European Symposium on Research in Computer Security (ESORICS), Annual Computer Security Applications Conference (ACSAC), Computer and Communications Security (CCS), ACM Symposium on Access Control Models and Technologies (SACMAT), Conference on Availability, Reliability

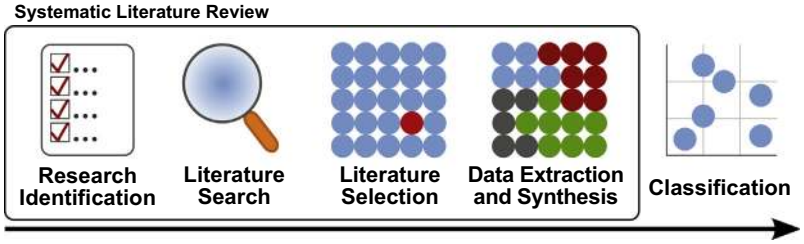

Fig. 1. Research methodology.

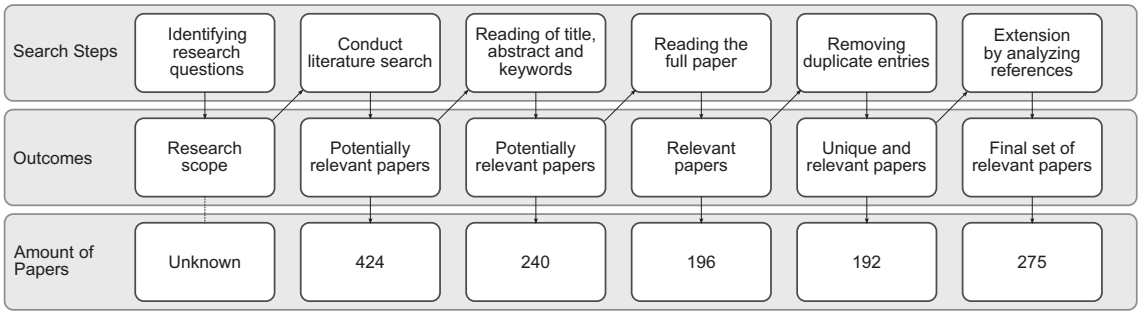

Fig. 2. Literature search and selection process (following [10,11]).

and Security (ARES), and Symposium on Policies for Distributed Systems and Networks (POLICY)) between 2004 and 2012 were examined. These publication venues were selected because they are top ranked publication media in PAIS or security research. If the context of publications related to *PAIS* (*business processes* or *workflows*) *and security* research they were identified as potentially relevant. In total, 424 papers were found (cf. Fig. 2).

2.3. Literature selection

Selection Criteria. Given the result set of all searches, our next task was to select relevant literature. We analyzed the publications according to the following scheme (cf. Fig. 2): In a first step, the title, abstract, and keywords were analyzed for relevance of content. Generally, it is expected that authors use terms such as *security* or similar in the titles or keywords. Instead, titles were often not expressive enough to identify them as PAIS *and* security relevant. Often, authors used names of specific research areas of security (e.g., access control) in the title. In fact, most of the literature could only be categorized by reading the full paper. Hence, in a second step, the contents of the publications were investigated. If the papers' content related to *PAIS and security* (or a related area of security) then the publication was identified as relevant literature. This manual decision process was guided by the decisions from the first step. Hence, articles investigating an area of security in PAIS (e.g., authorization in business processes) were also identified as relevant. For example, the publication [12] is about authorization in PAIS and, therefore, assesses a subfield of information security *and* is in the context of PAIS. Publications that concentrate only on one research area, either on PAIS or on Information Security, were excluded. These selection criteria narrowed down our results to 196 publications on security in PAIS.

Extension and quality assessment. In case of duplicate publications, i.e. articles published in conference proceedings and journals, we selected the journal articles and excluded the proceedings because journal articles usually extend the proceedings version. PhD thesis were excluded because the main results are often published in journals or proceedings of the investigated research field.

Additionally to the primary search results, we investigated the *references* (i.e. backward snowballing) in the publications to identify relevant literature that has been not been found in the primary search process (e.g., [13,14]). If publications complied with the selection criteria then they were identified as relevant literature. By investigating the references, we found a lot of additional publications to the primary literature searches. An explanation for this could be that only few publications actually use the general term "security"; instead they name specific areas e.g., access control or constraints.

In case of publications of the year 2012, we manually investigated proceedings and journal databases for relevant literature published in 2012 (retrieving date: 10/01/2012). However, it might be possible that not all conference proceedings or journal articles of 2012 were at that time available due to publishing delays. Hence, this survey may contain a subset of publications issued in 2012. This search process results in a set of 275 publications between the years 1993 and 2012. Please refer to Appendix A for a list of all publications. In the following, the data extraction and synthesis are based on this result set of publications.

2.4. Data extraction and synthesis

The main challenge was to classify the publications into a meaningful and solid structure. The *data extraction and synthesis* consisted of two stages and resulted into a set of 5 *categories* and 12 *security controls*; Fig. 3 displays the stages of the data extraction and synthesis.

In the first stage, the publications were categorized and grouped together as *security controls*. This step is similar to coding in qualitative data analysis (e.g., [15]). We used a tabular data extraction form that included a (1) full biographical reference of the publication, (2) date of the extraction, (3) reviewer name, and (4) name and (5) description of the main security idea. For each publication, we examined the title, abstract, and keywords, investigated the publications' central idea, and identified the area of security research in PAIS. We assume that authors want to indicate the papers' main idea by choosing suitable titles. Hence, to identify the

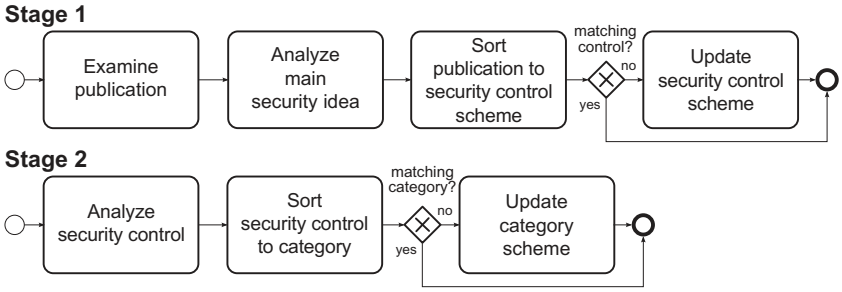

Fig. 3. Data extraction and synthesis: building a category scheme.

Table 1
Reference set of keywords.

Security control	Keywords
Security concepts	
Engineering	e-Business, engineering, information security, business process engineering, business process management, integration, management, risk
Modeling	BPMN, business process models, constraints, inter-organizational, model, modeling, multilevel, Petri Nets, requirements, UML
Security Requirements	Analysis, requirements, security requirements
Authorization and access control	
Access Control Models	Access control, authorization, delegation, model, RBAC, role-based, roles, task-based
Constraints	authorization constraints, constraints, enforcement, policies, process constraints
Applications	
Access Control Applications	Access control, application, authorization, flexible, framework, health, management, modeling, policy-based, RBAC, system, web
SOA Applications	Access control, authorization, architecture, attacks, BPEL, collaborative, framework, modeling, model-driven, policies, service-oriented, SOA, web service
Verification	
Consistency, Correctness, and Compliance	Binding, checking, constraints, consistency, context, data-flow, information, model-checking, models, mutual-exclusion, policies, verification
Monitoring	Monitoring, compliance, constraints, violations
Process Mining	Audit, anomaly, conformance checking, information, policies, process executions, process mining, RBAC
Failure handling	
Exception Handling	Exeption, execption handling, risk, patterns
Recovery and Repair	Dynamic, recovery, regeneration, specification, attacks
General Terms	Business processes, secure, security, workflows, workflow system

main idea of a publication, we analyzed the title using an automated term extraction tool. For example, the title of [16] uses the terms "authorization" and "model" and can be categorized as security control *Access Control Models*. In cases where term extraction did not extract suitable terms for categorization, the authors analyzed keywords and abstract to identify the central idea of each paper. Table 1 displays a reference set of keywords for each security control (cf. Section 3.3). General terms, i.e. terms that were found in most titles, such as business processes and workflows are listed at the bottom of the table. Furthermore, it can be seen from Table 1 that some keywords appear in more than one security control such as constraints. This is not surprising as, for example, *Constraints* are a security control (cf. Section 3.3.2) but are also monitored in the security control *Monitoring* (cf. Section 3.3.3). Hence, this shows that this classification can be complex due to ambiguities and potentially multiple mappings.

In the second stage, the controls were aggregated and synthesized into *categories*. Hence, we build a category scheme using similar techniques as in systematic mapping studies (e.g., [10]). In this literature review, each publication is only assigned to a control once. We set this restriction to obtain a concise and comprehensive structure. The complete set of controls is described in Section 3.3.

Alternative methods for classifying literature were considered but did not match the intent of our survey. For example, to classify a publication into two or more research areas of security would need a different approach. The assignment of the percentage a paper relates to one area and to another can be cumbersome due to ambiguities to extract relations.

To verify the manual classification, we reviewed how text mining approaches can be applied in systematic reviews [**?**]. However, we were not able to find a mining tool that exactly met our requirements such as parsing of PDF files and classifying into categories based on a reference set of keywords. In order to experiment with a tool, we selected the Konstanz Information Miner (KNIME) and used the text processing plug-into validate the categorization [18,19]. In particular, we adapted the document classification example (http://tech.knime.org/document-classification-example) and classified the abstracts of all publications in four steps: data preprocessing (e.g., punctuation erasure, case converter), keyword extraction (15 keywords per publication), transformation into a binary vector, and classification (using a support vector machine (SVM)) (cf. [19]). However, the results were not satisfactory and more of experimental type due to several reasons. First, the similarity of terms in categories (shown in Table 1 such as access control, constraints) can indicate that a categorization can become more difficult i.e. a manual classification or supervision is required. Secondly, the classification analyzes the frequency of terms of the abstracts. Some publications (e.g., from earlier years) might not include a high number of the most important terms in the abstract and are therefore not correctly classified. Moreover, some technologies have emerged or have gained more attention during the years (e.g., web services, SOA). Hence, the technological change also influenced the vocabulary used in the publications. Furthermore, contrary to an automatic classification, a manual classification incorporates semantic and domain knowledge (e.g., [20]). For example, manual or automatic searches for systematic reviews brought up overlapping and diverging results (e.g., [21]). Hence, tool support for an automated classification is currently not provided as we would require a detailed specification such as keywords for certain categories or multiple assignments of keywords to categories.

2.5. Classification of security controls

After identifying the main research areas (i.e., security controls) in PAIS, we want to further investigate these results in order to identify research challenges. Candidates for classification schemes were, for example, aspects of distribution (e.g., intra- or inter-organizational), life cycle phases, legal or regulatory restrictions, architectural aspects, or action types (cf. [22]). We chose life cycle phases and types of security actions because they were the most fitting categories for classifying security research in PAIS.

Therefore, we categorized all discovered security controls along the process life cycle and in terms of security actions (cf. Section 4): The process life cycle can be viewed as a cyclic process with four phases: design, enactment and execution, evaluation, and change (adapted from [1]). Secondly, security controls can be classified by their actions: prevention, detection, or reaction controls; a holistic security approach contains methods for all three actions (cf. [22]). Hence, with this classification, we expect to identify research challenges of security in PAIS. Other classification schemes for controls could be by nature e.g., physical, technical, procedural, and legal, or by orientation e.g., people, technology, and operations.

However, the classification for types of actions is for a holistic security approach more suitable.

In conclusion, the research methodology comprises of the following steps: First, we defined research questions and then, we performed an extensive literature search including horizontal and vertical searches. The third step was to select literature relevant for both security and PAIS. Moreover, publications were synthesized to a set of security controls. Lastly, these controls are classified by the process life cycle phases and action types.

3. Results

In the following, we will discuss the results of our systematic literature review. First, we will outline the publication sources and years of the selected publications. Secondly, we will examine definitions of security in PAIS literature. Then, we will display current security controls (i.e., countermeasures). Furthermore, we classify the controls along the process life cycle and by types of actions to determine research challenges and limitations.

3.1. Overview of selected publications

In this section, we will outline the publication years and sources of the selected literature.

3.1.1. Publication years

Fig. 4 displays the amount and type of articles on security in PAIS published between the years 1993 and 2012. As can be seen from the figure, the historical trend shows that publications on security in PAIS have increased constantly over the years. In the beginning, between 1993 and 1997 were only 0–3 publications each year. From 1998 until 2004, there were about 6–12 publications each year. Starting in 2005, there were about 16–39 publications each year. The year 2008 stands out because there were 39 publications on security in PAIS centering on access control models (and delegation) and their application in PAIS. Another reason could be the increased interest in SOA. In particular, the specifications of the Web Service Business Process Execution Language (WS-BPEL) 2.0 [23] and of the BPEL4People extension [24] were released in 2007. This led to a higher amount of publications on BPEL and related security concepts. To sum up, this development shows that security in PAIS is pursued by the scientific community and an emerging topic in PAIS. Hence, with the increasing interest on security in PAIS, a survey which provides an extensive analysis and examination of previous research becomes even more necessary.

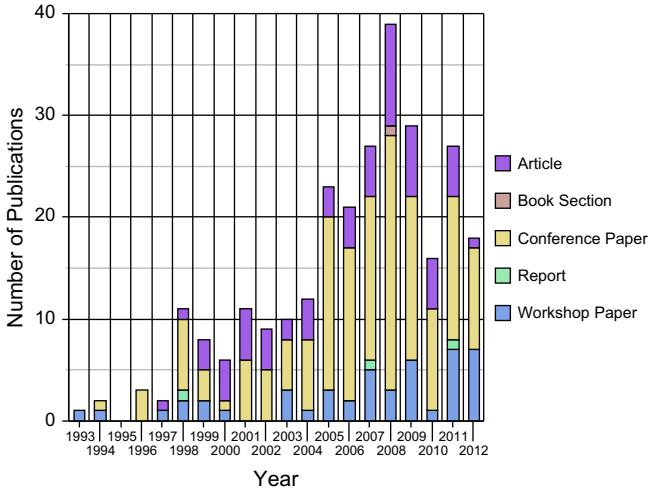

Fig. 4. Publications on security in PAIS between the years 1993–2012.

3.1.2. Publication sources

Furthermore, Fig. 4 displays the sources of publications. Overall, 76 percent of the publications were published in conference proceedings (161 papers) or workshop proceedings (46). Table 2 displays a list of the most frequent venues. Furthermore, 23% of the articles (64) were published in journals. The journals, in which the articles were most frequently published in, are shown in Table 3. Tables 2 and 3 display the name of the journal or venue and the number of papers. They list sources with at least two publications. The remaining one percent of papers was published as book Sections (1) or reports (3).

One reason for the increased number of workshop proceedings could be that multiple workshops on security in PAIS were hold in recent years, for example, the workshop on Security in Business Processes at the BPM conference (e.g., [25]).

3.2. Security in Process-Aware Information Systems

In this section, we tackle research question Q1 based on the literature review. As PAIS are Information Systems (IS), it is important to review state of the art of security in IS mainly referred to as information security. As our intention is not to provide a holistic view on the topic, we want to initially integrate views on security from this well-developed discipline (e.g., [26]). Specifically, information security is the protection of information an d information systems often related to as preservation of confidentiality, integrity, and availability (cmp. [27]). An extensive set of definitions of information security can be found in standards and recommendations such as the ISO/IEC 27000 standard or NIST Special Publications. For example, the ISO/IEC 27000 standard family specifies that information security *"is the preservation of confidentiality, integrity, and availability of information"* [28, p.3] but also notes that further requirements such as authenticity, accountability, non-repudiation, and reliability can be involved. Additionally, information security definitions can be found in regulations and law worldwide. For example, information security *"means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide [...] integrity [...], confidentiality [...], and availability [...].* according to federal law of the United States (44 U.S.C. Section 3542 (2012)).

From these definitions, it can be seen that security is about the protection of information and often security requirements such as confidentiality or integrity are utilized.

In general, PAIS differ from other Information Systems (IS) with respect to their behavioral aspect, i.e., the execution of a possibly large number of process instances based on a given process schema or template. Consequently, security requirements that are specific for PAIS can result from the dynamic behavior of process instances. First of all, for the verification of processes, dynamic soundness notions such as being free of deadlocks can play an important role for security, but also threats to the execution behavior such as initiating a huge number of process instances in order to block the system (denial of process execution). Further on, constraints that restrict the behavior and execution during runtime are vital for process security. (Dynamic) separation of duties, for example, demands for deciding for an appropriate actor not before runtime of the process instance. Secondly, PAIS are active systems, i.e., executing processes, invoking services and including users. This and the variety of aspects of such as system open the door for security threats, e.g., corrupting data that is exchanged by the PAIS and an invoked service. Even worse, if one aspect of the process has to be adapted, the side effects on the other process aspects have to be taken into consideration in order to avoid security problems. One example is the deletion of an actor in the organizational (RBAC)

Table 2
List of venues (with more than one publication).

Venue	No.
International Conference on Cooperative Information Systems (CoopIS)	17
ACM Symposium on Access Control Models and Technologies (SACMAT)	15
International Conference on Business Process Management (BPM) Workshops	11
International Conference on Business Process Management (BPM)	9
International Conference on Availability, Reliability and Security (ARES)	8
International Conference on Web Services (ICWS)	8
International Conference on Advanced Information Systems Engineering (CAiSE)	7
Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec)	6
European Symposium on Research in Computer Security (ESORICS)	6
Annual Computer Security Applications Conference (ACSAC)	5
European Conference on Web Services (ECOWS)	4
International Conference on Model Driven Engineering Languages and Systems (MoDELS)	4
Symposium on Applied Computing (SAC)	4
International Conference on Services Computing (SCC)	4
International Conference on Database and Expert Systems Applications (DEXA) Workshops	3
International Symposium on Policies for Distributed Systems and Networks (POLICY)	3
International Conference on Availability, Reliability and Security (ARES) Workshops	2
International Conference on Business Information Systems (BIS)	2
Working Conference on Business Process Modeling, Development, and Support (BPMDS)	2
International Conference on Computational Intelligence for Modelling, Control and Automation (CIMCA)	2
International Conference on Risks and Security of Internet and Systems (CRiSIS)	2
International Conference on Database and Expert Systems Applications (DEXA)	2
International Conference on Enterprise Information Systems (ICEIS)	2
International Conference on Service-Oriented Computing (ICSOC)	2
International Conference on Web Engineering (ICWE)	2
Modellierung	2
IFIP TC-11 International Information Security and Privacy Conference (SEC)	2
International Conference on Web Information Systems (WISE)	2
IEEE Computer Security Foundations Workshop (CSFW)	2

Table 3
List of journals (with more than one publication).

Journal	No.
Journal of Computer Security	7
Computers & Security	3
Information Systems	3
Data & Knowledge Engineering	2
Electronic Commerce Research	2
Electronic Notes in Theoretical Computer Science	2
Information and Software Technology	2
Information Management & Computer Security	2
Journal of Network and Computer Applications	2
ACM Transactions on Information and System Security (TISSEC)	2
IEEE Transactions on Services Computing	2
IEEE Transactions on Systems, Man, and Cybernetics	2

model which leads to an empty set of authorized actors for a certain process activity during runtime [29].

In the next step, we will examine how security is defined in PAIS literature. Although research acknowledges the importance of security in PAIS [5,30–33], the definition of what security means particular in PAIS remains unbalanced and centers on four different aspects. First, the definition and development of security policies is important for the design and execution of processes. For example, a secure workflow is defined in [33, p. 35] as a *"computer supported business process that is capable to against security threats and further satisfies the security policies defined by the workflow modeler"*. According to [34, p. 131], a secure workflow system is a system *"that protects enterprise data according to a workflow security policy"*. In [35, p. 200], security *"is concerned with the ability to enforce a security policy governing the disclosure, modification or destruction of information"*. In [36, p. 10], security policies *"must ensure many properties: integrity, authorization, availability, confidentiality, authentication and separation of duty"*. Moreover, in [37, p. 43] it is stated that an *"important approach for managing security is represented by the development of policy-based security services in order to provide security operations relevant to business processes"*. As can be seen from these definitions, security requirements are often used to support the definition of security policies. For example in [38], security is defined with the requirements: confidentiality, integrity, and availability. These definitions show that often security in PAIS is based on security policies, i.e., a *"overall intention and direction as formally expressed by management"* [28, p. 4]. These policies define the protection of information (e.g., data) and ensure specific requirements (e.g., confidentiality).

Furthermore, security in PAIS is often related to authorization and access control mechanisms. For example, [39, p. 288] states that *"the key to secure implementation of WFMS is proper authentication and authorization of participants in a workflow process"*. WFMS signifies Workflow Management System. Security *"involves the implementation of access control security mechanisms to ensure that task dependencies are coordinated and that tasks are performed by authorized subjects only"* is defined in [40, p. 1]. Further, [41, p. 509] states that for security it is important *"to verify the correctness of the workflow authorizations against the organization's security policies and the actual execution environment before or even during any real execution of the workflow"*. Hence, access control mechanisms are necessary to ensure that only authorized subjects can execute processes. These authorization mechanisms often rely on organizational security policies (e.g., organizational models, job descriptions, and security guidelines).

In addition, security in inter-organizational process scenarios is defined in [42, p. 73]: *"Inter-workflow security is concerned with the security of the communication and cooperation of autonomous workflow systems, running at different units of the same organizations or at different organizations"*. Surprisingly, this was the only definition relating to the secure interconnection between processes of one or more organizations. Considering computing architectures such as grid computing (e.g., [43]) a secure exchange is even more important.

This literature review shows that definitions of security in PAIS are unbalanced; they display only one view but leave out other

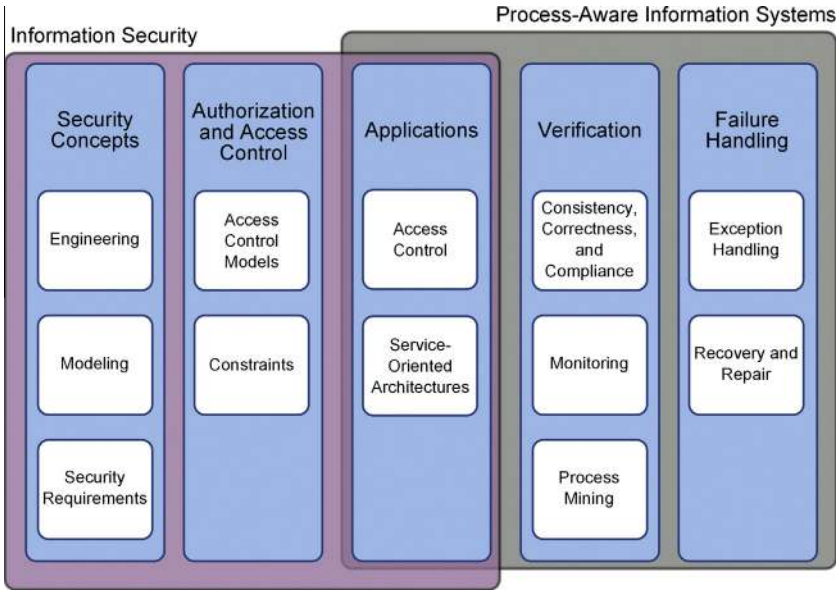

Fig. 5. Categorization of existing security controls in PAIS.

aspects such as aspects of processes, humans, and life cycle phases (e.g., design time and run time aspects). It seems that a broader security definition in PAIS is needed to emphasize all characteristics of PAIS (cmp. Section 5). Based on this finding, we will carefully investigate current security countermeasures (i.e. security controls) in PAIS in the next section.

3.3. Security controls

In this section, we examine research question Q2 to investigate currently utilized security controls in PAIS. Based on the literature review (cf. Section 2), we found a set of 12 security controls (i.e., countermeasures) described in PAIS literature which could be further classified into five categories as depicted in Fig. 5. Two general observations can be made. At first, literature rates security an important factor in BPM and PAIS in general. Secondly, security in PAIS constitutes an interdisciplinary research area combining research from information security with research from PAIS and BPM. Typical controls from the PAIS domain are, for example, compliance and process mining techniques. Example controls from the information security discipline are e.g., access control models and security requirements. Further, it can be seen that traditional boundaries are crossed. Specifically in the category *Applications*, principles from both research domains are applied.

The first category *Security Concepts* comprises security controls typically used when modeling and engineering business processes. As an example, we can name extensions to process modeling notations such as BPMN [44,45] that enable the annotation of security-relevant information to process models. Another category is *Authorization and access control* and refers to all mechanisms that manage the authorization of users in a PAIS. Thereby, access control constitutes the predominantly applied control measure in research, academic and commercial PAIS, and practice nowadays [46]. Role-based access control models, for example, use roles (e.g., job functions) as a set of permissions in order to restrict access. Moreover, additional constraints are often imposed on the processes to support further security controls such as authorization constraints. The third category refers to *Verification* of business processes and all related aspects. Thereby, correctness, consistency, and compliance play an important role for PAIS security since in cases of incorrect or non-compliant process executions security problems such as unauthorized access might occur. This holds true for all phases of the process life cycle. At process design time, the specification of relevant security and compliance constraints should be consistent and correct i.e., no conflicts with other constraints and the process models must exist. Certain constraints might be not verifiable until run time such as synchronization constraints or constraints referring to time. These constraints have to monitored during process run time [47,48]. Finally, the a posteriori verification of process executions against compliance and security constraints at evaluation time is addressed by process analysis and mining techniques [49]. Category *Failure Handling* refers to the handling of exceptions and errors during process execution time. Without an appropriate treatment, exceptional situations can lead to severe security problems such as unauthorized access. Exception handling strategies comprise recovery or repair techniques that put process instances back into consistent execution states, e.g., by compensation or applying process adaptations [50,51]. Lastly, the area *Applications* subsumes case studies and implementations of security features in PAIS, particularly focusing on Service-Oriented Architectures (SOA), access control models, and academic and commercial PAIS implementations.

Some security controls might relate more to each other than others. For example, often authors provide *Modeling* concepts using *Security Requirements* in their publications. Further, we found that *Access Control Models* and *Constraints*, *Access Control Models* and *Access Control Applications*, and *Correctness, Consistency, and Compliance* and *Monitoring* were closely related. As each paper was only assigned once to a category, these relationships are not displayed in Fig. 5.

Fig. 5 provides a comprehensive overview of currently investigated security controls in PAIS. Nonetheless, further emerging topics can be easily integrated in terms of additional controls and categories. To underpin the coverage of PAIS literature in our study we also evaluated the categorization schema of Fig. 5 along the six key concerns in Business Process Management (BPM) as discussed in [6]: (1) process modeling languages, (2) process enactment infrastructures, (3) process model analysis, (4) process mining, (5) process flexibility, and (6) process reuse. Key concern (1) is well covered by category *Security Concepts*. (2) stretches over categories *Authorization and Access Control*, *Applications*, *Verification*, and *Failure Handling*, since all these categories refer to security at

process run time. We will further classify the five security categories presented in Fig. 5 along the process life cycle in Section 4 where process enactment constitutes one of the phases. Use cases (3) and (4) are covered by category *Verification* with the corresponding analysis methods from process mining and correctness checks. (5) corresponds to category *Authorization and Access Control* since a few papers address possible security problems in the sequel of applying process changes [52,46]. (6) is the only category that has not been dealt with by existing approaches in the context of security in PAIS.

The following sections describe each category together with its security controls in detail.

3.3.1. Security concepts

The first category *Security Concepts* addresses the incorporation of security aspects into business processes at their design time. It consists of three security controls: *Security Engineering* refers to methods for building secure systems and reference architectures. The second control is *Modeling* and centers on modeling notations and languages that support the integration of security-relevant information into process models. Lastly, security objectives of PAIS and their usage in the business engineering context are examined in *Security Requirements*.

Security Engineering. This control refers to the overall process of defining, establishing, enforcing, and evaluating security in PAIS, more precisely, addressing *"the management of the whole business process life cycle in conformity with security and dependability objectives [...]"* as defined by [53, p. 459]. In order to achieve this goal, at first, a business process strategy concerning security is formulated [53]. Security countermeasures are modeled together with the business processes. Further on, the business processes are evaluated concerning their security costs (investment, operating, and recovery costs) based on security reference processes. Lastly, security countermeasures (safeguards) are selected and monitored. Another approach to measure security in the engineering phase is to elicit security requirements. These security requirements are often specified based on business processes [54–56] to identify threats and vulnerabilities and to define security measures based on an analysis of stakeholders, risks, and business environment [57]. A methodology to transfer paper-based business processes into automated secure workflows is shown in [58]. In addition, a methodology for incorporating security requirements and attackers into the development of business processes is presented in [59]. A later section provides an in-depth analysis of security requirements in PAIS.

Modeling. Security control *Modeling* comprises means to include security-related information into business processes at design time. Note that in this section we summarize efforts of security-specific elements and notations. Basic access control and authorization mechanisms are elaborated on in Section 3.3.2. In general, existing process modeling notations do not include security-related patterns such as security controls or requirements (e.g., confidentiality). However, recently security patterns have been developed for the following business process modeling notations: Event-driven Process Chains (EPCs), Business Process Modeling Notation (BPMN), Unified Modeling Language (UML), and Petri Nets. EPCs are enriched with security function symbols, such as message level encryption, end-to-end-encryption, and access control [60]. In BPMN, extensions enable the modeling of security requirements [44,45] and task-based entailment constraints [61,62] such as separation of duties. Most security patterns are defined in the context of UML. SecureUML [63], for example, is a UML-based modeling language that enables the specification of access control information in the design of application models to derive (RBAC-related) security policies [64]. Other UML extensions support the annotation of security-relevant information, such as security requirements in [65–67] or location constraints for mobile business processes [68]. In [69], security-relevant information is identified from UML-based business process models to derive access control policies. Furthermore, the explicit modeling of multi level security [35,32] and security functions [70,71] has been shown for Petri Nets. In addition, a language for modeling security requirements is proposed in [72]. Moreover, an overview on business process security modeling in terms of compliance is provided in [73].

Security Requirements. Security requirements (also known as security objectives) are standard principles to enforce security in information systems (IS). The most common requirements for IS are, for example, confidentiality, integrity, and availability (cf. [27]). Security in PAIS can be evaluated by determining the security requirements as contribution to the intended security level of the PAIS. Basically, research distinguishes security requirements for business processes [38,74,53] and for workflow systems [30,5,31]. The most frequently examined security requirements are *Integrity, Confidentiality, Authentication, and Availability*. Additionally, a lot of objectives to secure intellectual property (e.g., *Copyright, Originality*) were found. Notably, the requirements *Security management and administration* in [5], *Audit* in [31], *Safety* and *Reliability* in [53] were only indicated once. Moreover, [75,76] support the identification and specification of security requirements in SOA-oriented workflow systems. The framework in [75,77] uses requirements engineering to develop secure business processes and further to derive secure business constructs executed in Web Services Business Process Execution Language (WS-BPEL): The early requirements engineering phase consists of the analysis and identification of actors and their dependencies, delegation authorities, and trust relationships. The later requirements engineering phase consists of defining functional and non-functional requirements.

3.3.2. Authorization and access control

In general, security research in PAIS centers on authorization and access control. In PAIS, the function of access control is to manage which process participants (e.g., users, services) have access to which resources (e.g., tasks, process instances) by respective authorization artifacts and mechanisms (cf. Fig. 6). Authorization is expressed based on organizational knowledge often represented by access control models and process constraints [12].

Access Control Models. There are currently three major types of access control models in PAIS. The first is role-based access control that restricts access based on roles and permissions. Secondly, task-based authorizations are used to specify access rights depending on tasks. Lastly, multi-layered security models define authorizations based on security levels (e.g., public, secret, confidential). In addition, access control models are often enhanced with a dele-

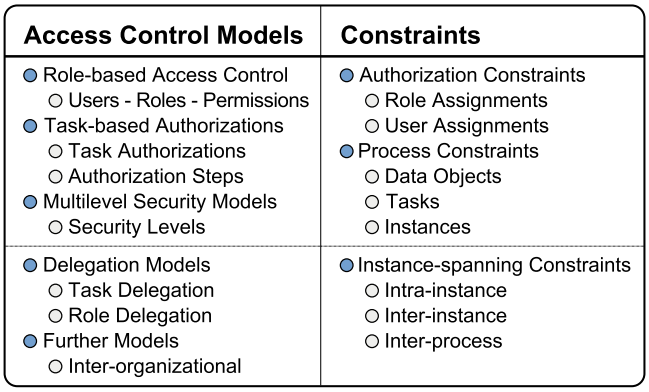

Fig. 6. Authorization and access control artifacts in PAIS.

gation function. Due to the multitude of delegation models, we aggregate these models in a separate section. Additionally to access control models, an overview on how resources are utilized and allocated in terms of authorization are defined as workflow resource patterns in [78].

Role-based Access Control. The most frequently adopted model to manage access control is the Role-Based Access Control (RBAC) model (e.g., [79,80]). To restrict access, the model uses the concept of roles that consist of permissions. A permission is an authorization to do a certain action such as executing a task. Users (i.e., subjects) can be associated with one or more roles. Roles can be hierarchically structured where e.g., sub roles inherit the permissions of the super roles. In Fig. 7, for example, two roles *Doctor* and *Nurse* specialize role *Staff*. Two users *Steve* and *Beth* are associated to role *Nurse*. Different options to assign users to tasks exist. The assignment of process tasks to users is accomplished via role assignments as depicted in a). For executing task *T1*, for example, users must have role *Doctor*. The assignment can be resolved based on the organizational model, i.e., user *Molly*. Other process notations such as BPMN feature an assignment based on swimlanes (cf. http://www.omg.org/bpmn/Samples/Elements/Swimlanes.htm) as illustrated by b in Fig. 7).

In addition to standard RBAC models, further models have been developed incorporating PAIS-specific elements such as process tasks or instances. For example, the concept of tasks (i.e., activities) is used in [81–83]. Thereby, roles are often associated with tasks in order to define which users (having roles) are authorized to execute them and authorization constraints on the process. On the other hand, the Workflow RBAC model (W-RBAC) [12] integrates the concepts of workflow cases (instances) associated with users and permissions to specify authorizations. Additionally, organizational units where a user can be member or head are defined. Furthermore, flexibility and adaptivity is a key concern in recent models. For example, RBAC models supervising control flow changes such as adding or deleting tasks are displayed in [84,52]. The Adaptive Workflow RBAC (AW-RBAC) model manages authorized control flow, data flow, administrative, and service changes in [85]. An extension of the AW-RBAC model in [46] enables security by integrating responsibilities (a mix of structural and data restrictions).

Task-based Authorization Models. Task-based authorizations are based on single tasks (e.g., signing a form). For example, the Workflow Authorization Model (WAM) in [16] grants only an authorization to perform a certain task during the actual execution of the task. The access rights are granted when the tasks starts and revoked when it completes. Furthermore, task-based authorizations controls use authorization steps to manage authorizations in [86–88]: An authorization step is a single piece of work (e.g., granting a signature) and abstracts a related set of permissions. First, a trusted user has to invoke and grant an authorization step. In case, the authorization step is granted, a set of permissions is enabled. Authorizations have a usage, validity, and expiration characteristics.

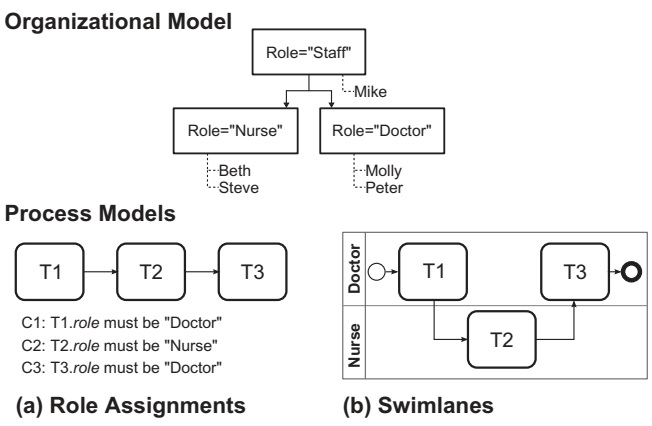

Fig. 7. Example process models with access control structures.

Multilevel Security Models. Multilevel secure (MLS) workflow models specify security levels (e.g., confidential, secret, or public) for processes or tasks to define authorization levels. Especially high-to-low dependencies have to be avoided, for example, confidential (i.e., high) tasks should not be followed by public (i.e., low) tasks. For example, the MLS model in [89,90] associates tasks with various security levels (e.g., from confidential to public levels). Inter-level task dependencies are evaluated regarding security policy conflicts such as the information flow between confidential and public tasks. In case of confidential tasks are followed by public tasks, the tasks are only executed by trusted participants. Another MLS model in [32] analyzes data (information flow) dependencies (i.e., high-to-low writings or low-to-high readings) associated with tasks. Furthermore, MLS models in [91,92] divide, depending on the security-level, each process further into single-level workflows (e.g., one process for confidential tasks and one for public tasks). Moreover, a multi-layered state machine specified in [33] separates various aspects of control in a process for analyzing the flow of authorizations. For example, integrity and authorization are assured when a user has the privilege to execute a task and rights are revoked after task completion.

Delegation Models. In PAIS, delegation refers to transferring authority to execute a certain process task by an authorized participant to another participant. Delegation authorizations can be specified for tasks of a single process instance or for all instances of a process type. Delegation can become a security issue in PAIS: if users are delegating tasks to other users not having the appropriate qualifications or security level to execute the task, security violations can occur such as unauthorized access. One delegation model proposed in literature is the Delegation Workflow RBAC model (DW-RBAC) [93] that extends the W-RBAC model with the specification and revocation of delegations. It provides delegation rights of generic tasks (for all instances) and of specific tasks (single instances). The Delegation Authorization Model [40] extends the WAM by introducing delegation authorization templates. An extension [94] of the secure workflow model [33] supports task delegation and revocation. In [95], the authority to delegate depends on the risk of delegation based on three security levels. In case of high risk, only the least capable task-role (the weakest role to execute a task) can be delegated or in case of low risk, more powerful roles can be delegated. In addition, capability-based delegation is investigated in [96]. Moreover, transfer delegations i.e., a delegator transfers its permissions completely to a delegatee, are utilized in [97].

Further Models. In addition to the discussed access control models, a broad range of access control models have been developed for specific domains in PAIS such as inter-organizational processes or service-oriented-architectures. For example, an inter-organizational access control model in [98] integrates an entity *role domain*. Each organization maps its organizational structure to one role domain. Tasks are associated with specific roles depending on the role domains. Furthermore, organization-based access control [99] is used to administer access control in inter-organizational processes in [36,100]. Moreover, access control models in [101,102] support an automated model-driven development in service-oriented environments.

In conclusion, a very large, still increasing number of access control models is provided for PAIS. Most RBAC models base on the NIST RBAC Standard Model [80] and extend it with certain functionality (e.g., delegation, process adaptation, or administra-

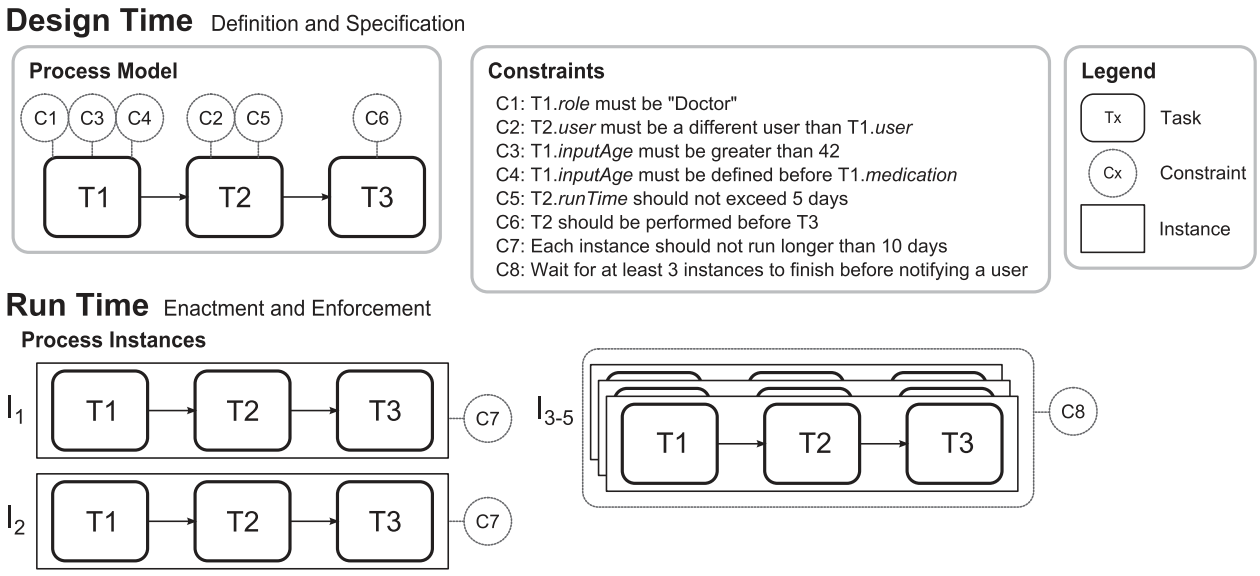

Fig. 8. Design and run time aspects of constraints in PAIS.

tion) or include certain process-related entities (e.g., tasks, cases, or organizational units). Hence, with this proliferation of contributions it seems that the area of access control is thoroughly covered.

Constraints. In PAIS, certain authorization information cannot be expressed solely based on access control models which requires the definition of additional authorization constraints [103]. Moreover, in previous PAIS literature, authorization constraints have been often used to directly specify role or user assignments in case no access control model exists. In general, authorization constraints can be distinguished into constraints on (1) *role and user assignments* (authorization) and on (2) *processes* (i.e., tasks, process instances) (cf. Fig. 6). Examples for (1) comprise separation and binding of duties constraints [104,103]. An example for a separation of duty constraint is `C2` as provided in Fig. 8. Separation of duty is a security principle that disseminates privileges to multiple users to fulfill an objective and further reduce fraud and errors [105]. For example, to approve a large `creditRequest`, two *seniorAccountants* have to perform task `approveCredit` to sign the approval. In recent years (and due to the strong development of RBAC as de facto standard), the definition of separation of duty (also known as four-eyes-principle) and binding of duty constraints as authorization constraints has gained increased interest.

[103] provides a categorization of authorization constraints in PAIS into static constraints (enforced at design time; e.g., `C1` in Fig. 8), dynamic constraints (enforced at run time; e.g., `C7`), and hybrid constraints (design and run time; e.g., `C2` in Fig. 8). [106] defines authorization constraints as active rules. Thereby, instance (for tasks and instances), temporal (for time frames), and history (the last execution state of a task or instance) authorization constraints can be specified.

Moreover, specific characteristics of authorization constraints in PAIS are investigated in literature. For example, [107] shows that the satisfiability of a process model in a certain access control state remains intractable only when enforcing simple constraints. Also resiliency, a property of the system where the workflow completes even with some unavailable users, is examined. The satisfiability of workflow systems while delegating tasks is examined in [108].

Additionally to authorization constraints, further restriction of access might become necessary with respect to time or data (cf. Fig. 6). An example could be that a certain task is to be only executed by a user having a role X in a certain time frame each day. Such additional restrictions can be expressed by (2) process constraints (see Fig. 6), i.e., constraints on process aspects such as data objects, process tasks, process instances restricting the access with respect to time or data [109,110,46,111]. As in general such constraints can be used for synchronization, compliance, or temporal monitoring (cf. [110]), they are also useful to enforce security controls. Particularly, synchronization between the execution of different process instances has been identified as security-critical issue in [12,112]. Think, for example, of a scenario where the credit sum over all process instances, i.e., for all customers, must not exceed a certain amount. Existing approaches addressing such instance-spanning constraints only consider certain scenarios. The W-RBAC model [12] defines (a) *inter-case constraints* and (b) *reciprocal separation of duties*: Inter-case constraints (a) enable the specification of constraints to different instances, for example, the number of times a task was executed by a user. Reciprocal separation of duties (b) signify that e.g., if user *Bob* signs a request after *Alice*, *Alice* cannot sign the (next) request after *Bob*. Moreover, the logic-based approach in [112] gives an overview on resource, data, and time constraints for inter-instance constraints. The first approach towards a more holistic definition of inter-instance constraints is provided by [113] based on a framework and classification for intra-instance (i.e., enforcement in single instances, see Constraint `C7` in Fig. 8), inter-instance (i.e., multiple instances, see `C8`), and inter-process (i.e., multiple processes) constraints.

In conclusion, constraints either restrict authorization or enforce limits on e.g., tasks or process instances. As most research centers on authorization constraints to enforce security, other constraints such as data and timing constraints should be also considered. For example, if a certain task has not been executed within a certain amount of time, suitable responsive actions should be started to support the process e.g., delegate tasks. Moreover, most approaches center on the enforcement of constraints in single process instances and only few consider inter-instance and inter-process settings. Note that in this section existing approaches on defining security-relevant constraints in PAIS have been discussed. Section 3.3.3 will provide a discussion on existing approaches to check, monitor, and enforce constraints in PAIS.

3.3.3. Verification

This section provides an overview of verification methods such as consistency, correctness, and compliance that apply to security in PAIS. Business process compliance signifies that the enactment

of business processes complies with a set of norms such as standards (e.g., ISO/IEC 27000) or regulations (e.g., Sarbanes–Oxley Act (SOX)) [114]. As discussed in Section 3.3.2, a frequently investigated norm is separation of duty, e.g., imposed on a credit application that has to be checked by two accountants (one has to be a senior accountant) before they can approve a credit. Depending on which information a norm is referring to and which process information is available, the verification can take place at process design time, run time, or analysis time [115]. Separation of duties, for example, has to be checked at design time (i.e., at least two accountants (one has to be senior) are in the organization) but also during process execution (i.e., at least two accountants (one has to be senior) are currently available). Design time compliance checks require the presence of a process model [116]. Run time compliance checks are generally referred to as compliance monitoring [47] and might become necessary in case the process model is not available or accessible. Checking compliance after finishing process execution (ex post) is mainly accomplished by applying process mining techniques [117]. Altogether, compliance violations can be security critical since they might lead to unexpected behavior of the process (e.g., long running processes) or vulnerabilities (e.g., loopholes in the access control system) which further might be exploited by threats. In the following, we first discuss existing approaches on consistency, correctness, and design time compliance checks before continuing with monitoring and process mining approaches.

Consistency, Correctness, and Design Time Compliance. Process execution has to be conducted in a correct manner in order to avoid potential security problems resulting from situations such as deadlocks or reaching abnormal process states. Many notions and checks for ensuring correctness of process execution referring to structure and behavior exist [1]. Compliance can be seen as a correctness notion regarding the process semantics [118]. In addition to these correctness aspects, it is necessary to ensure correctness and consistency for the security-relevant constraints imposed on the process models as well. Respective checks are generally performed at *design time* and ensure the consistency and correctness of constraints. First, security policies such as organizational policies are verified for their consistency. For example in [119], process executions and organizational security policies are compared by transforming processes and policies into a common constraint language and then are compared and evaluated for inconsistencies. Other approaches, verify constraints for consistency and correctness such as authorization constraints [120–122,104,123] or information flow policies [124]. For example in [120], based on a workflow authorization schema and task-based authorization constraints (e.g., separation of duties), rules are specified to ensure constraint consistency and conflict-free constraints. If constraints conform to these rules, a sound workflow schema is established. Furthermore, the consistency of authorization constraints in SOA-based environments is verified by model checking approaches in [125–127]. Moreover, the effects of organizational changes (i.e., changes in authorization constraints) have been examined in [29].

Monitoring. Monitoring refers the active supervision of norms during process execution and the reactive or proactive alert in case of violations such as unauthorized access of data, exceptional behavior, or blockage of processes. [48] distinguishes the following monitoring approaches: *Automaton-based monitoring* investigates compliance violations using an automaton for checking imposed rules (e.g., [128,47]). In general, an automaton verifies rules and reaches certain states (e.g., satisfied, violated). *Logic-based monitoring* applies logical formalisms in order to detect compliance violations such as in [129,130]. *Violation pattern-based monitoring* approaches analyze execution paths for the existence of certain anti-patterns (violation patterns) [131,132]. It has to be emphasized that in certain scenarios, monitoring services cannot build on information about the process model such as in business process choreographies or Enterprise Resource Planning (ERP) applications. In these cases, typically, the communication is managed based on events. For example, in SOA-based environments, monitoring commonly supervises the states of services. In case a service in a web service composition has a uncertain state, a monitor repairs the faulty process [133]. Hence, with the use of stateful activities, information about running activities is acquired, monitored, and independently repaired.

Process Mining. Relevant to security considerations, process mining techniques analyze and extract process-related information from (process) event logs. Process mining can be used to (1) discover processes without utilizing any a priori knowledge and (2) to check for conformance by comparing the existing process model with its model derived from event log [117]. In [49], for example, the process model and its process executions are examined in order to detect inconsistencies based on discovering anomalous process executions that may stand for security violations such as low-level intrusion or fraud [49,134,135]. Service behavior is checked for conformance in [136]. Furthermore, the conformance of process logs with policies such as RBAC policies is examined in [137] or data flow policies in [138]. In [138], specifically, process execution logs are verified with data flow policies to evaluate the information flow between three security levels (i.e., secret, confidential, and public). In fact, the authors investigate whether the information flow directs only from the public to the confidential or the secret domain but not e.g., from the secret to the public level. Moreover, conformance checking of authorization, temporal, and data constraints using process mining is presented in [139]. Further mining techniques discover organizational models (which can be further adapted to RBAC models) using organizational mining [140] or staff assignment mining [141]. The suitability of mining techniques to derive RBAC models is analyzed in [142]. Furthermore, delta analysis of RBAC models compares a predictive RBAC model with a current-state RBAC model in order to detect security violations [143]. Additionally to process mining, a business provenance model for tracking and correlating the important aspects of business operations is shown in [144,145]. In this approach, relevant information on data, resources, and executed tasks are captured to address specific compliance or performance goals or to find compliance violations and their root causes.

3.3.4. Failure handling

Handling failures and recovering processes is essential to the reliability and stability of a PAIS. [146] identifies workflow engines, activities, and communication failures as potential failure sources in workflow systems as well as two types of failures in PAIS: system and semantic failures. If deviations from normal process executions arise, these deviations are called *exceptions* [147]. In case exception handling fails, actions to recover processes have to be considered. If these mechanisms do not catch deviations, unexpected behavior or vulnerabilities can be exploited.

Exception Handling. There are three approaches on handling exceptions, namely the pattern-based, rule-based, and case-based management of exceptions. The first approach described in [147] specifies workflow exception patterns for exception handling capabilities in PAIS. In fact, five exceptions types are defined: work item failure, deadline expiry, resource unavailability, external trigger, and constraint violation. These types are managed either at task level or process instance level. Refer to http://workflowpatterns.com/patterns/exception/ for an extensive review on exceptions in PAIS. Case-based reasoning (e.g., [50]) captures exception handling strategies of occurred exceptions to reuse them in similar, new, and abnormal situations. In rule-based approaches, rules are specified to manage if, for example, common errors occur. Event condition action (ECA) rules are used in [148] to specify

data-dependent, workflow-dependent, and time-dependent rules. Another example in [149] integrates additional exception handling functionality such as compensation into process models. In service-oriented environments, data guards monitor data and raise exceptions in case of violations in [150,151].

Recovery and Repair. Recovery is an ultimate action to restore a process from an unknown/unexpected to a normal execution state. In literature, there are three methods to recover processes. First, recovery mechanisms often remedy the effects of a failure with an *action or a set of actions* (e.g., [149,147]). For example in [147], three recovery actions "no action", "rollback" (i.e., backward recovery), and "compensate" (i.e., forward recovery) are proposed to diminish effects of exceptions. In case of *rollback*, the effects of preceding tasks leading to an exception or affected by an exception are reversed into a consistent state. In case of *compensation*, adequate compensation tasks or alternatives are defined beforehand (if possible) to recover the process. Another recovery method are *ad hoc changes* where the process instance is modified in order to work out exceptions. For example, ad hoc recovery in [152] is specified by adapting the structure of processes instances in case of exceptions or ad hoc events. In addition, in [153], a self-adaptive recovery net (an extended Petri net model) adapts the structure at run time to manage exceptions such as task-based and region-based recovery policies such as skipping, redoing or compensating tasks. System recovery through dynamic regeneration of workflow specifications is shown in [154,155]. In the long run, ad hoc changes that appear more frequently have to be evaluated if these changes should be permanently adapted to the process model i.e., by process evolution. The last recovery action is to *repair* the running process. For example, an approach for monitoring and repairing workflows (web service compositions) using stateful activities is displayed in [133]. The recovery of the effects of malicious tasks that have been executed in PAIS is shown in [156]; an intrusion detection system is used to recognize malicious tasks. Then, the system automatically examines all control flow and data flow dependencies of the affected tasks and tries to repair the effects such as redoing a task. A repair algorithm after malicious attacks is also presented in [157]. Ensuring task dependencies and restoring consistency by removing the effects of partially executed malicious tasks is shown in [158].

In literature, we found that the terms *evolution* and *ad hoc changes* are often synonymously used even though only ad hoc changes were actually referred to. Whereas ad hoc changes enable a change in a running process instance and do not change the underlying process model, process evolution modifies the process models and running process instances might be adapted using migration strategies. It is important that these two terms are not mixed.

3.3.5. Applications

As a major part of research, the practical application of concepts such as access control models is an important matter. Specifically in this category, it can be seen that the concepts of the security and PAIS domain are combined and deployed in applications. The first part centers on applications in service-oriented architectures such as web service compositions. The last part of this section discusses applications of access control models. In order to fully understand the purpose of this section, it is important to discuss the commonalities and differences between web service security and security in PAIS. Web service compositions constitute processes and (complex) web services at the same time. Hence, on the one side, common security requirements such as integrity exist. On the other side, also differences between both worlds arise, for example, from the different degree of human involvement. Aside specific extensions to web service compositions such as BPEL4People [24], web service compositions are typically fully automatic and do not involve human actors. By contrast, the human involvement in the execution of business processes can range from fully human (e.g., patient treatment) to zero human (as for web service compositions). As a conclusion, an additional requirement for process-oriented applications in addition to "pure" web services is authorization [159]. Authorization is often tackled by means of organizational structures/ RBAC mechanisms together with additional policies such as separation of duty. Hence, our goal is not to fully outline web service security but to outline the means necessary to enable security in service-oriented PAIS.

Service-Oriented Architectures. We divide our results into three aspects of service-oriented PAIS: access control mechanisms, web service compositions, and web-based attacks. The first aspect is the integration of access control mechanisms and constraints in service-oriented architectures (SOA). For example, the WS-BPEL extension BPEL4People [24,160] integrates organizational functions such as separation of duty constraints or manual task assignments and is developed as a service in [161]. Authorization constraints in WS-BPEL in [162] and an access control framework for Business Processes for Web Services (BPEL4WS) in [163,164] provide authorization in SOA. The second aspect are web service compositions that are secured by additional parameters (constraints) to verify certain security restrictions (e.g., compatibility, encryption). For example in [165], each task in a process is associated with a web service and security constraints in a (secure) web service composition. Security constraints can either be defined by the requester and are needed for the interaction between two web services (compatibility constraints). At execution time, the WS-BPEL web services are interconnected with regard to security parameters. Furthermore, the approach in [166] integrates a container called "process slip" comprising data, audit data, security policies, and a workflow description. The process slip is used to transfer security-related information (e.g., access control) between web services in a composition. In another example [167], the workflow execution path is based on collaboration policies (e.g., authorization constraints, security requirements for interaction level) that state under which circumstances a collaboration is allowed. Web services that do not comply with these terms are not used and replaced. As a special case of web service compositions, inter-organizational processes are frequently examined in literature. Inter-organizational workflows are deployed between two or more partner organizations which require appropriate security controls to manage the exchange of security-sensitive information between multiple partners (e.g., [168,169]). For example in [169], a secure document flow, context dependent access constraints, and application domain specific security extensions are used to provide security. Moreover, a comprehensive reference architecture for Security as a Service in [170] complements the approach by integrating model-driven security engineering. The third aspect are web-based attacks by exploiting vulnerabilities. A methodology to analyze vulnerabilities of SOA in [171] starts with an analysis of a point of view (e.g., a business process) and continues with evaluating attack effects, active components, involved standards, and triggering properties. A classification of attacks in SOA-based workflows in [172,173] defines attacks and countermeasures for BPEL workflow engines such as a stateful BPEL firewall in [174].

Access Control. Not only the modeling but also the application of access control models (cf. Section 3.3.2) is important in research. For example, an implementation of the WAM is displayed in [175] and of W-RBAC in [176] (cf. Section 3.3.2). Other implementations center on domain-specific implementations such as the application of RBAC in flexible systems in [177,178], in e-health systems in [179,180], and in event-driven activity management systems in [181]. Further approaches use wrappers to route access through a layer in [182] and autonomous objects to authenticate and authorize users in [183].

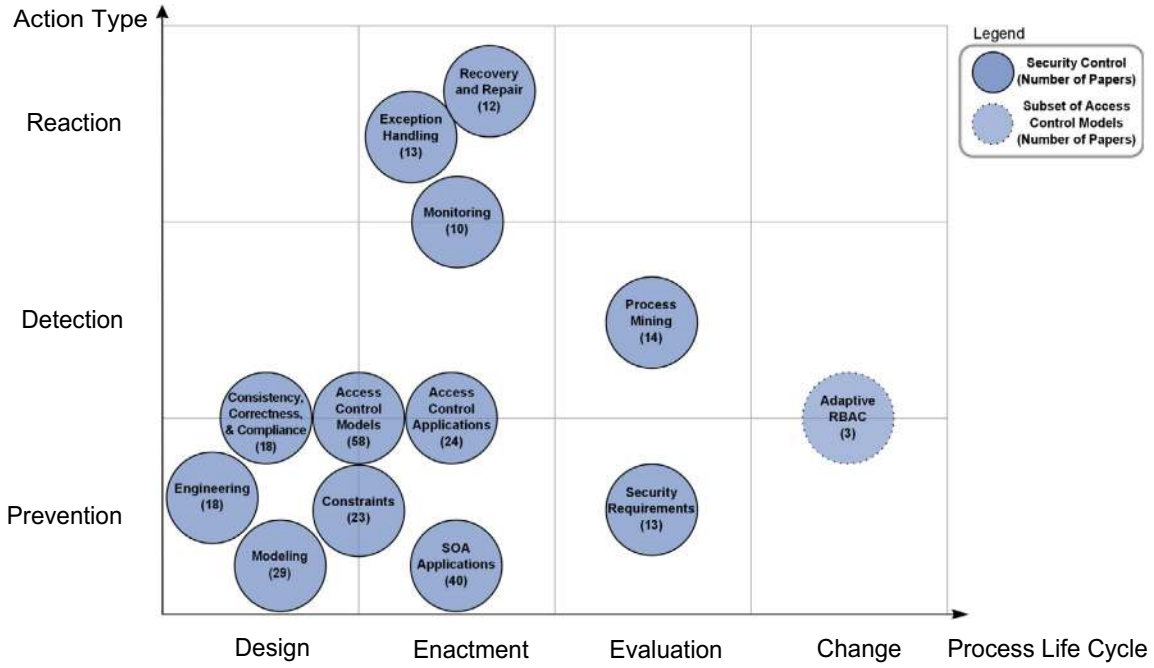

Fig. 9. Classification of controls.

In conclusion, based on the literature review, we discovered a rich set of security controls in PAIS which can be classified into 5 categories. These categories show that security in PAIS is an interdisciplinary research area with influences from PAIS and information security.

4. Classification of security controls

In the following, we classify the controls (defined in the previous section) into (Q3.1) which process life cycle phases they are utilized and (Q3.2) which type of security actions they support in order to get a holistic view on security in PAIS. With this comparison, we expect to identify key security research in PAIS and further to discover research challenges and gaps.

The process life cycle can be viewed as a cyclic process with four phases: design, enactment and execution, evaluation, and change (adapted from [1]). In the `Design` phase, the processes are identified, modeled, and validated. Note that the workflow design is often based on business process design. Afterwards, the workflows (i.e., automated processes) are enacted and executed within the `Enactment` phase. Based on the process schema, process instances are created and executed, each representing a single use case. Then, the process traces are reviewed and evaluated within the `Evaluation` phase. Outcomes of the phase might result in optimizations of processes and process changes in the `Change` phase. Furthermore, security methods can be classified by their type of action: prevention, detection, or reaction; a holistic security comprises controls for all three types (cf. [22]). Typically, preventive countermeasures stop someone from doing something, for example (adapted from [22]), electronic article surveillance (EAS) on merchandise aims at preventing shoplifting from retail stores. Furthermore, methods to detect security violations should exist, for example, a detection system at all store exits alarms the staff when someone with EAS-attached merchandise passes through. Moreover, responsive methods react on detected violations. As an example take the staff members to check the person, who set off the alarm, for stolen merchandise.

The classification of the security controls collected and discussed in Section 3.3 along the dimensions "Process Life Cycle" and "Action Type" is shown in Fig. 9. The horizontal axis contains the phases of the process life cycle (design, execution, evaluation, change) and the vertical axis classifies the security controls by their action: prevention, detection, or reaction. Please note that the number below each security control states the amount of papers related to that topic. *Modeling* security-related information in process models, for example, is part of the `Design` phase and a preventive security countermeasure. *Access Control Models* are more difficult to classify; these models are specified at design time and enacted at run time. In that, they not only provide preventive controls to define authorization policies but also include controls for detection, i.e., they typically restrict access to unauthorized users. The controls *Access Control Models, Consistency, Correctness, and Compliance, Constraints*, and *Access Control Applications* are often interrelated and are therefore connected in Fig. 9. *Adaptive RBAC* is a subset of *Access Control Models*. We divide the research cluster to show that three RBAC models authorize adaptations (cf. Section 3.3.2) and display the adaptive RBAC models separately in the `Change` phase. *Exception Handling* and *Recovery and Repair* are linked because they are often interrelated in research. As *Monitoring* refers to the active supervision of norms during process execution, the detection of norm violations, and support of controls to reduce violations, it is assigned to the `Enactment` phase as detecting and reactive countermeasure.

Q3.1: Is security enforced in every phase of the process life cycle?

As can be seen from Fig. 9, by far the most preventive security controls have been established in the `Design` and `Enactment` phase. In fact, 51% of the literature is concerned with the `Enactment` (139.5[1] papers) phase. The `Design` phase accounted for 38% (105.5). `Evaluation` contained 10% (27) of the publications and `Change` only one percent (3). This indicates that current security controls center on the `Design` and `Enactment` phase and leave

[1] The number of papers has a decimal place due to the grid shape of the classification. For example, the number of papers of the security control *Access Control Models* is divided by four to assign a set of publications to each area.

out the Evaluation and Change phase. Nevertheless, for a holistic security approach, *all* phases should be considered.

It can be also seen from Fig. 9 that some security controls show a higher amount of related papers than others. For example, *Access Control Models* have been investigated by 61 publications (*Access Control Models* (58) and *Adaptive RBAC* (3)). By examining the literature (cf. Section 3.3.2), we can identify that certain aspects of access control are widely elaborated such as RBAC or delegation in RBAC. Although a vast amount of publications exist, not all aspects of access control models are covered. For example, literature centers mostly on certain features of RBAC models such as process-related concepts (e.g., W-RBAC [12]). However, the management of access control for external services (e.g., web services) that are invoked during process execution, for example, has been only considered in [85]. Hence, the existence of certain controls in the classification does not signify that sufficient research exists leaving no research gaps. On the contrary, we believe that security in PAIS is an emerging topic and that most of the publications center on very specific aspects. Hence, even controls with a fair amount of publications in the classification should still be considered for research.

Q3.2: Which types of security controls are utilized in PAIS?

The classification in Fig. 9 displays that most publications center on preventive security controls; currently fewer controls for detection and reaction exist. In fact, 63 percent (174.5 papers) of literature provided preventive measures. Detection measures accounted for 26 percent (70.5) and reaction for only 11 percent (30) of security in PAIS research. Most literature was found in the areas Prevention/Design (82) and Prevention/Enactment (78). On the other hand, no literature was found for the Reaction areas Design, Evaluation, and Change. Hence, it can be concluded that reaction countermeasures are yet not fully incorporated in PAIS. The areas Detection/Design, Detection/Enactment, Detection/Evaluation, Detection/Change, Prevention/Evaluation, and Prevention/Change show only a few assigned publications (between 3 and 13). This result could be obtained for various reasons. First, the literature review was not extensive enough to obtain suitable results. This cannot withstand as an extensive literature review was performed including vertical and horizontal searches (cf. Section 2). Another reason is that current research on e.g., reaction measures exist but the conducted survey only selected publications related to PAIS *and* security. Thus, research on reaction countermeasures was not included in the survey if it was not related to PAIS *and* security. Hence, controls with few assigned publications signify that research has mostly not been centering on PAIS *and* security. Moreover, we conclude that all areas with no or few associated entries are emerging research areas, can be identified as research challenges, and are subject to future work.

5. Research challenges

This section identifies current research challenges in security research in PAIS based on the literature review and the classification in the previous section (inspired by [184]). The challenges displayed in Fig. 10 are categorized by perspective. First, standardization challenges center on the agreement of terminology and use of technology (such as the use of standards); this category includes *Agreement on Terminology and Controls* and *Consistency with Related Fields and Standards*. Secondly, technical challenges focus on the technical measurement, deployment and evaluation of security controls in PAIS. Technical challenges are *Measurement*, *Testing*, *Evaluation*, *Detection Controls* and *Reaction Controls*. Finally, human challenges include the involvement of humans in the development and use of security controls (cf. *Human Orientation*). As reaction controls can incorporate implementation features such as run time monitors but also may include end users reaction strategies (e.g., resolving exceptions). Hence, reaction controls are categorized as technical and human challenge. In the following, we will describe each challenge briefly.

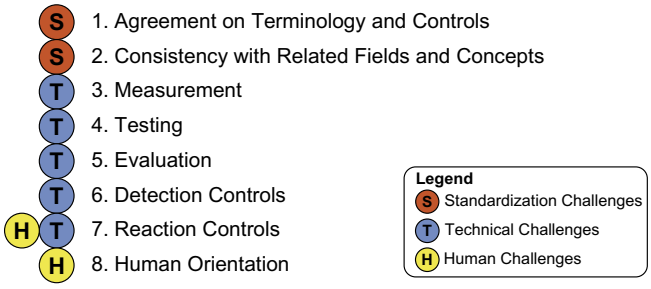

Fig. 10. Research challenges.

Agreement on Terminology and Controls. In general, research acknowledged the importance of security in PAIS e.g., [5,31] but the definitions on security in PAIS are unbalanced (cf. Section 3.2). Hence, there is no common agreement on what security means in PAIS literature. Nevertheless, research often refers to security but does not specify its meaning; in turn, literature often focuses on certain aspects e.g., confidentiality. This paper constitutes a first step towards reaching a common consensus as in this literature review, we analyzed security definitions in PAIS research and compared these with definitions with legal and international standards (cf. Section 3.2). In addition, we examined state of the art of security controls in PAIS. This should further support the development of an agreement on the definition of security in PAIS.

Consistency with Related Fields and Standards. As stated in previous sections, security in PAIS constitutes an interdisciplinary research area (cf. Fig. 5) that adapts concepts from research on information security and PAIS. Surprisingly, most PAIS literature does not refer to any standards or recommendations. Only the proposed NIST standard for RBAC [80] is well-recognized in PAIS research (cf. Section 3.3.2). However, a variety of standards and recommendations for information security exist such as ISO/IEC 27000 and the NIST special publications. For example, the ISO/IEC 27000 standard family displays security techniques for requirements, code of practice, implementation guidance, measurement, and audit in information security management systems. Advances and further developments can be achieved by taking these standards and recommendations into consideration in PAIS research as well.

Measurement. Current research proposes solutions on how to secure PAIS but does not state how these concepts can be measured, e.g., with respect to security requirements and controls. As stated before, well-developed recommendations and standards for the measurement of security exist in other security areas. For example, the ISO/IEC 27004 provides guidelines how to assess the effectiveness of control objectives and controls. Future work may adapt these measurements to PAIS and define a set of metrics for a security assessment.

Testing. Current PAIS research and practice provide theoretical results on certain aspects, but often abstain from providing information on how these concepts can be tested. To our best knowledge, techniques for PAIS to test certain security requirements are only presented in [139]. As previously stated, recommendations from related fields are merely addressed, although there exist a variety of guidelines for security testing. For example, the Open Source Security Testing Methodology Manual (OSSTMM) http://www.isecom.org/research/osstmm.html provides a rich set of methods for security testing and analysis. Further examples are

the NIST special publications that center on e.g., early software testing (NIST SP 800-142) and information security testing (NIST SP 800-115). Future research should consider which techniques are suitable for PAIS and how these techniques can be adapted to PAIS.

Evaluation. Current PAIS research centers mostly on ex-post evaluation of security in PAIS by applying process mining techniques (e.g., [49,135,139]). Here, the question arises if and how security level assessment in PAIS can be conducted also at design and run time. Hence, design time and run time procedures for evaluating e.g., static or dynamic security controls should be considered for future work. Again it should be noted that standards exist that could support the evaluation process e.g., the common criteria for IT security (i.e., ISO/IEC 15408).

Detection Controls. To the best of our knowledge, current research and practice does not investigate the detection of security attacks in PAIS during run time. So far, research centered on detecting anomalous process executions ex post (cf. Section 3.3.3). However, it would be beneficiary to be able to react on such anomalous executions in time, i.e., at run time. Typical systems to detect security incidents are intrusion detection systems that monitor occurring events and analyze them for possible incidents (e.g., violations or threats of violation of policies) [185].

Reaction Controls. It is essential for a secure system, to react to security violations or attacks in order to keep a secure state of the system. So far, responsive controls in PAIS have been only provided in the area of failure handling such as exception handling and recovery and repair of processes. However, the aim is not only to respond to security violations at run time but also to respond to security violations that are identified at design time e.g., during process modeling. For example, guidelines to resolve e.g., constraint conflicts can be introduced (e.g., [29,186]) or runtime monitors that apply corrective enforcement techniques can be deployed (e.g., [187]). Reaction controls in PAIS may be controlled by autonomous, intelligent agents that react based on observations (e.g., sensors) or by humans. So far, research on security in PAIS centers on the technical side, but should consider also human aspects for reactions controls e.g., by clearly describing all options how to solve a violation. Furthermore, it is important to prevent, detect, and react to attacks in PAIS. So far, research has not centered on how to react to attacks. Reaction controls in PAIS are therefore a key challenge.

Human Orientation. Security in PAIS literature centers mostly on technical aspects. However, humans are an important factor when it comes to security. For example, humans design processes and execute tasks. Social engineering attacks, for example, entail physical (e.g., workplace, Internet) and psychological aspects such as human nature and emotions (cf. [188,189]). Hence, a holistic security approach also includes the involvement and awareness of humans. Therefore, current research often misses to evaluate or investigate human-related aspects such as awareness and comprehension of process participants. For example, BPMN security extensions are empirically investigated with end users for comprehensibility in [190] and a set of symbols for security extensions in business processes is produced in [191]. Another example are reaction controls. Current PAIS assume that users may/can resolve (security) violations themselves but often, the comprehension of violations (e.g., described in a error message or log file) are not evaluated with humans. Hence, humans should be considered especially for the design of reaction controls e.g., when resolving security violations. Options should be clearly described to facilitate the decision of humans.

To sum up, these research challenges show that security in PAIS is still a challenging research field. This set of challenges does not claim to be exhaustive and was derived from the literature review and classification. As security in PAIS is interdisciplinary research, we expect that new challenges will emerge from an interdisciplinary perspective.

6. Discussion

Based on the previous section, we will discuss principal findings, potential impact on research and practice, future directions, and limitations of this review.

6.1. Main findings

This literature review shows that security in PAIS is a challenging topic in PAIS. Surprisingly, we found that definitions of security in PAIS are unbalanced and often contain security policies, security requirements, authorization and access control mechanisms, or inter-organizational scenarios. Additionally, we identified 12 security controls in the area of security concepts, authorization and access control, applications, consistency, correctness and compliance, and failure handling in PAIS. Furthermore, we detected research challenges and limitations.

To our best knowledge, this is the first systematic literature review on security in PAIS. Previous research has centered only on certain (interrelated) aspects of security. For example, the review in [73] examines compliance support for business process security modeling. The authors review current modeling techniques to display e.g., security requirements or authorization constraints. In this paper, we review current process modeling techniques as part of security controls (cf. Section 3.3.1). Another review in [192] examines state of the art of RBAC models in information security literature and examines RBAC models for workflow systems. The review discovers 64 RBAC models. We found 60 access control models in this study. A reason for this could be that the search in [192] was performed automatically and ours manually. Due to our extensive search strategy (cf. Section 2.2), quality assessment, and extraction review process, we think that the different number may be resulted because of different reasons. Our data extraction and synthesis process examined publications by the main idea proposed in the paper. If the paper focused mainly on authorization constraints in relation to RBAC models it was added to the category *Constraints*. In doing so, publications could have been assigned to category *Constraints* and not to *Access Control Models*. Further reviews center on certain aspects of security or enabling security can be a side effect of these aspects in PAIS e.g., control flow or change patterns such as [193,194]. Altogether, none of these reviews centers on a holistic approach on security in PAIS.

6.2. Impact on research and practice

The aim of this paper was to investigate security in PAIS by examining current research and practice of security in PAIS. Due to the extensive amount of literature on security in PAIS and the missing understanding and use of terminology, the review of publications on security in PAIS is cumbersome and time consuming. This literature review provides the first comprehensive investigation of security in PAIS. The results of the literature review, as shown in Fig. 5, are a set of 5 categories and 12 clusters that help determine and categorize security research in PAIS. It shows that it is an interdisciplinary field which may support researchers when considering future security research in PAIS.

Another major result of this review is the classification of security controls in PAIS. The classification shows that past research has centered on the design and enactment phase of the process life cycle and on preventive controls (cf. Fig. 9). With this knowledge in mind, future research may be directed to different phases (e.g., evaluation) or controls such as reaction controls. Hence, the classification indicates a number of future research challenges and directions (cf. Section 5) for both researchers and practitioners.

For example, the most challenging fields seem to be the design and development of detection and reaction controls in PAIS.

In addition, practitioners may use this review for revisiting security approaches in PAIS. For example, by providing an overview of existing security controls in PAIS, practitioners may adapt controls to existing PAIS in order to enhance security. Furthermore, practitioners may use the classification shown in Section 4 as a reference to determine if the utilized PAIS (or IS) applies a holistic security approach. Then, supportive actions to enable security in the utilized PAIS can be taken. Also, this classification can be used to assess PAIS (or IS) for security.

6.3. Limitations of this review

This review investigated security in PAIS. Therefore we performed a systematic literature review (cf. Section 2). Due to the multitude of publications centering on security and/or PAIS, we decided to only select literature which contained a main idea from the area of security and PAIS to narrow down our results. Security literature that did not discuss implications on PAIS (e.g., implementation) was excluded. Vice versa, PAIS literature that did not contain any security concepts (e.g., confidentiality, security requirements) was not selected.

Topics that are often associated with security (e.g., due to related concepts) such as compliance or exception handling have been explained in previous sections. However, as an extensive elaboration would go beyond the scope of this paper, we refer the reader to more a detailed elaboration in the referred literature in the sections.

7. Conclusion

This systematic review aimed at investigating a holistic view on security in PAIS by tackling three main research questions. Therefore, we examined 275 publications between the years 1993 and 2012 and categorized these publications into 5 categories of security controls using a systematic mapping approach. Furthermore, to gain a holistic view on security in PAIS, we classified these controls along the process life cycle and by types of action. Lastly, based on the literature review and the classification, we identified research challenges. The main findings of this review are as follows:

- Q1. Literature shows that security in PAIS is an important topic but there was no common understanding of the definition of security in PAIS. We found that security definitions are unbalanced and often focus on specific aspects such as security policies, security requirements, authorization and access control mechanisms, or inter-organizational scenarios.
- Q2. We identified 12 security controls in the area of security concepts, authorization and access control, applications, verification, and failure handling in PAIS. These security controls show that PAIS research provides a rich set of measures to ensure security for certain aspects (e.g., access control).
- Q3. Security controls in PAIS can be found mostly as prevention measures for the design and enactment of processes (e.g., process modeling, access control models). Thereby they often center on static models and miss to include dynamic features such as process changes. Furthermore, only few detection and reaction controls exist but are important for a holistic security approach.

From our point of view, a major result is the classification of security controls in PAIS along the process life cycle and by types of action. This classification may indicate a number of future research challenges and directions as shown in Section 5 for both researchers and practitioners. The most challenging fields seem to be the design and development of detection and reaction controls. Furthermore, practitioners may use this review for rethinking security approaches in PAIS. Moreover, this review may support the development and selection of security controls for engineering PAIS.

In future work, we aim at working towards closing the gap between security research in Information Systems and PAIS. Further on, we will concentrate on some of the open issues outlined in this paper such as the development of detection and reaction controls. For example, we want to detect unauthorized access or misuse of permissions in RBAC models using process mining techniques. Furthermore, we want to investigate the evaluation of inter-instance constraints with mining techniques.

Appendix A. Supplementary material

Supplementary data associated with this article can be found, in the online version, at http://dx.doi.org/10.1016/j.infsof.2013.12.004.

References

[1] M. Weske, Business Process Management: Concepts, Languages, Architectures, Springer, 2007.
[2] T. Mather, S. Kumaraswamy, S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, Inc., 2009.
[3] R. Winter, R. Fischer, Essential layers, artifacts, and dependencies of enterprise architecture, J. Enterprise Architect. 3 (2006) 7–18.
[4] G. Müller, R. Accorsi, Why are business processes not secure?, in: Festschrift Prof. Johannes Buchmann, 2013.
[5] Workflow Management Coalition, Workflow Security Considerations – White Paper, Technical Report Document Number WFMC-TC-1019 Document Status - Issue 1.0, Workflow Management Coalition, 1998.
[6] W.M.P. van der Aalst, A decade of business process management conferences: personal reflections on a developing discipline, in: A. Barros, A. Gal, E. Kindler (Eds.), Proceedings of the 10th International Conference on Business Process Management (BPM), Lecture Notes in Computer Science, vol. 7481, Springer, 2012, pp. 1–16.
[7] B. Kitchenham, Procedures for Performing Systematic Reviews, Joint Technical Report, Department of Computer Science, Keele University and Empirical Software Engineering, National ICT Australia Ltd., 2004.
[8] B. Kitchenham, S. Charters, Guidelines for performing Systematic Literature Reviews in Software Engineering, EBSE Technical Report EBSE-2007-01 Version 2.3, School of Computer Science and Mathematics, Keele University and Department of Computer Science, University of Durham, 2007.
[9] H.M. Cooper, L.V. Hedges, J.C. Valentine, The Handbook of Research Synthesis and Meta-Analysis, Russell Sage Foundation, 2009.
[10] K. Petersen, R. Feldt, S. Mujtaba, M. Mattsson, Systematic mapping studies in software engineering, in: Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering (EASE), EASE'08, British Computer Society, Swinton, UK, 2008, pp. 68–77.
[11] R. Wendler, The maturity of maturity model research: a systematic mapping study, Inform. Software Technol. 54 (2012) 1317–1339.
[12] J. Wainer, P. Barthelmess, A. Kumar, W-RBAC – a workflow security model incorporating controlled overriding of constraints, Int. J. Cooper. Inform. Syst. 12 (2003) 455–485.
[13] S. Jalali, C. Wohlin, Systematic literature studies: database searches vs. backward snowballing, in: Proceedings of the ACM-IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), ESEM '12, ACM, New York, NY, USA, 2012, pp. 29–38.
[14] C. Wohlin, R. Prikladnicki, Systematic literature reviews in software engineering, Inform. Software Technol. 55 (2013) 919–920.
[15] M.B. Miles, A.M. Huberman, Qualitative Data Analysis: An Expanded Sourcebook, SAGE, 1994.
[16] V. Atluri, W.-K. Huang, An authorization model for workflows, in: Proceedings of the 4th European Symposium on Research in Computer Security (ESORICS), Springer, 1996, pp. 44–64.
[17] B. Kitchenham, P. Brereton, A systematic review of systematic review process research in software engineering, Inform. Software Technol. 55 (2013) 2049–2075.
[18] M.R. Berthold, N. Cebron, F. Dill, T.R. Gabriel, T. Kötter, T. Meinl, P. Ohl, K. Thiel, B. Wiswedel, KNIME – the konstanz information miner: version 2.0 and beyond, SIGKDD Explor. Newslett. 11 (2009) 26–31.
[19] K. Thiel, M. Berthold, The KNIME Text Processing Feature: An Introduction, Technical Report 120403F, KNIME.com AG, 2012.
[20] A.-H. Tan, Text mining: the state of the art and the challenges, in: Proceedings of the PAKDD 1999 Workshop on Knowledge Discovery from Advanced Databases, 1999, pp. 65–70.

[21] H. Zhang, M.A. Babar, P. Tell, Identifying relevant studies in software engineering, Inform. Software Technol. 53 (2011) 625–637.
[22] B. Schneier, Secrets and Lies: Digital Security in a Networked World, first ed., John Wiley & Sons, 2004.
[23] OASIS Web Services Business Process Execution Language (WSBPEL) TC, Web Services Business Process Execution Language Version 2.0, OASIS Standard, OASIS, 2007. <http://docs.oasis-open.org/wsbpel/2.0/OS/wsbpel-v2.0-OS.pdf>.
[24] A. Agrawal, M. Amend, M. Das, M. Ford, C. Keller, M. Kloppmann, D. König, F. Leymann, R. Müller, G. Pfau, et al., WS-BPEL Extension for People (BPEL4People), Specification 1.0, Active Endpoints Inc., Adobe Systems Inc., BEA Systems Inc., International Business Machines Corporation, Oracle Inc., and SAP AG, 2007. <http://public.dhe.ibm.com/software/dw/specs/ws-bpel4people/BPEL4People_v1.pdf>.
[25] R. Accorsi, R. Matulevicius, Workshop on security in business processes – a workshop report, Enterprise Model. Inform. Syst. Architect. 8 (2013) 75–80.
[26] R. Baskerville, Information systems security design methods: implications for information systems development, ACM Comput. Surv. 25 (1993) 375–414.
[27] R.J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, second ed., John Wiley & Sons, 2008.
[28] ISO/IEC 27000, Information technology – Security techniques – information security management systems – overview and vocabulary, Technical Report ISO/IEC 27000:2009, ISO/IEC, Switzerland, 2009.
[29] S. Rinderle-Ma, M. Leitner, On evolving organizational models without losing control on authorization constraints in web service orchestrations, in: Proceedings of the 12th IEEE Conference on Commerce and Enterprise Computing (CEC), IEEE Computer Society, Los Alamitos, CA, USA, 2010, pp. 128–135.
[30] R.A. Botha, J.H. Eloff, A security interpretation of the workflow reference model, in: Proceedings of the Information Security – From Small Systems to Management of Secure Infrastructures, vol. 2, 1998, pp. 43–51.
[31] V. Atluri, Security for workflow systems, Inform. Security Tech. Rep. 6 (2001) 59–68.
[32] K. Knorr, Multilevel security and information flow in petri net workflows, in: Proceedings of the 9th International Conference on Telecommunication Systems – Modeling and Analysis, Special Session on Security Aspects of Telecommunication Systems, Dallas, TX, 2001, pp. 9–20.
[33] P.C.K. Hung, K. Karlapalem, A secure workflow model, Proceedings of the Australasian Information Security Workshop Conference on ACSW Frontiers 2003, Vol. 21, Australian Computer Society, Inc., 2003, pp. 33–41.
[34] D.L. Long, J. Baker, F. Fung, A prototype secure workflow server, in: Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC), IEEE Computer Society, 1999, p. 129.
[35] V. Atluri, W.-K. Huang, An extended petri net model for supporting workflows in a multilevel secure environment, in: Proceedings of the 10th IFIP WG 11.3 Working Conference on Database Security (DBSec), 1996, pp. 199—216.
[36] S. Ayed, N. Cuppens-Boulahia, F. Cuppens, Deploying access control in distributed workflow, Proceedings of the 6th Australasian Conference on Information Security, vol. 81, Australian Computer Society, Inc., Wollongong, NSW, Australia, 2008, pp. 9–17.
[37] F. Giraldo, M. Blay-Fornarino, S. Mosser, Introducing security access control policies into legacy business processes, in: Proceedings of the 15th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW), IEEE Computer Society, Helsinki, Finland, 2011, pp. 42–49.
[38] S. Röhrig, K. Knorr, Security analysis of electronic business processes, Electr. Commerce Res. 4 (2004) 59–81.
[39] E. Gudes, M.S. Olivier, R.P.v.d. Riet, Modelling, specifying and implementing workflow security in cyberspace, J. Comput. Secur. 7 (1999) 287–315.
[40] K. Venter, M.S. Olivier, The delegation authorization model: A model for the dynamic delegation of authorization rights in a secure workflow management system, in: Proceedings of the 2nd Annual Conference on Information for Security for South-Africa (ISSA), Muldersdrift, South Africa, 2002, pp. 1–12 (published electronically).
[41] Z. Yi, Z. Yong, W. Weinong, Modeling and analyzing of workflow authorization management, J. Network Syst. Manage. 12 (2004) 507–535.
[42] S. Wu, A. Sheth, J. Miller, Z. Luo, Authorization and access control of application data in workflow systems, J. Intell. Inform. Syst. 18 (2002) 71–94.
[43] J. Mangler, C. Witzany, O. Jorns, E. Schikuta, H. Wanek, I. Ul Haq, MobilegSET – secure business workflows for mobile-grid clients, Concurrency Comput. Pract. Experience 22 (2010) 2036–2051.
[44] A. Rodríguez, E. Fernández-Medina, M. Piattini, A BPMN extension for the modeling of security requirements in business processes, IEICE Trans. Informa. Syst. E90-D (2007) 745–752.
[45] M. Menzel, I. Thomas, C. Meinel, Security requirements specification in service-oriented business process management, in: Proceedings of the 4th International Conference on Availability, Reliability and Security (ARES), 2009, pp. 41–48.
[46] M. Leitner, J. Mangler, S. Rinderle-Ma, SPRINT-responsibilities: design and development of security policies in process-aware information systems, J. Wireless Mobile Networks Ubiquit. Comput. Depend. Appl. (JoWUA) 2 (2011) 4–26.
[47] F.M. Maggi, M. Montali, M. Westergaard, W.M.P. van der Aalst, Monitoring business constraints with linear temporal logic: An approach based on colored automata, Proceedings of the 9th International Conference on Business Process Management (BPM), vol. 6896, Springer, 2011, pp. 132–147.
[48] L.T. Ly, S. Rinderle-Ma, D. Knuplesch, P. Dadam, Monitoring business process compliance using compliance rule graphs, in: Proceedings of the 19th International Conference on Cooperative Information Systems (CoopIS), Lecture Notes in Computer Science, Springer, 2011, pp. 82–99.
[49] W.M.P. van der Aalst, A.K.A. de Medeiros, Process mining and security: detecting anomalous process executions and checking process conformance, Electr. Notes Theor. Comput. Sci. 121 (2005) 3–21.
[50] Z. Luo, A. Sheth, K. Kochut, J. Miller, Exception handling in workflow systems, Appl. Intell. 13 (2000) 125–147.
[51] S. Rinderle, M. Reichert, Data – driven process control and exception handling in process management systems, in: E. Dubois, K. Pohl (Eds.), Proceedings of the 18th International Conference on Advanced Information Systems Engineering (CAiSE), Lecture Notes in Computer Science, vol. 4001, Springer, 2006, pp. 273–287.
[52] B. Weber, M. Reichert, W. Wild, S. Rinderle, Balancing flexibility and security in adaptive process management systems, Proceedings of the 13th International Conference on Cooperative Information Systems (CoopIS), Lecture Notes in Computer Science, vol. 3760, Springer, 2005, pp. 59–76.
[53] T. Neubauer, M. Klemen, S. Biffl, Secure business process management: a roadmap, in: Proceedings of the 1st International Conference on Availability, Reliability and Security (ARES), IEEE Computer Society, 2006, pp. 457–464.
[54] T. Neubauer, J. Heurix, Defining secure business processes with respect to multiple objectives, in: Proceedings of the 3rd International Conference on Availability, Reliability and Security (ARES), IEEE Computer Society, Los Alamitos, CA, USA, 2008, pp. 187–194.
[55] T. Neubauer, J. Heurix, Objective types for the valuation of secure business processes, in: Proceedings of the 7th IEEE/ACIS International Conference on Computer and Information Science (ACIS), IEEE Computer Society, Los Alamitos, CA, USA, 2008, pp. 231–236.
[56] T. Neubauer, M. Pehn, Workshop-based risk assessment for the definition of secure business processes, in: Proceedings of the 2nd International Conference on Information, Process, and Knowledge Management (eKNOW), IEEE Computer Society, 2010, pp. 74–79.
[57] A. Zuccato, Holistic security requirement engineering for electronic commerce, Comput. Security 23 (2004) 63–76.
[58] S. Fritsch, V. Karatsiolis, M. Lippert, A. Wiesmaier, J. Buchmann, Towards secure electronic workflows, in: A. Atzeni, A. Lioy (Eds.), Proceedings of the 3rd European Public Key Infrastructure Workshop: Theory and Practice (EuroPKI), Lecture Notes in Computer Science, vol. 4043, Springer, 2006, pp. 154–168.
[59] M. Backes, B. Pfitzmann, M. Waidner, Security in business process engineering, in: Proceedings of the 1st International Conference on Business Process Management (BPM), 2003, pp. 168–183.
[60] M. Jensen, S. Feja, A security modeling approach for web-service-based business processes, in: Proceedings of the 16th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems (ECBS), 2009, pp. 340–347.
[61] C. Wolter, A. Schaad, Modeling of task-based authorization constraints in BPMN, in: Proceedings of the 5th International Conference on Business Process Management (BPM), Lecture Notes in Computer Science, vol. 4714, Springer, 2007, pp. 64–79.
[62] C. Wolter, A. Schaad, C. Meinel, Task-based entailment constraints for basic workflow patterns, in: Proceedings of the 13th ACM Symposium on Access Control Models and Technologies, SACMAT '08, ACM, New York, NY, USA, 2008, pp. 51–60.
[63] T. Lodderstedt, D. Basin, J. Doser, SecureUML: a UML-Based modeling language for model-driven security, Proceedings of the 5th International Conference on UML – The Unified Modeling Language, vol. 2460, Springer, 2002, pp. 426–441.
[64] D. Basin, J. Doser, T. Lodderstedt, Model driven security for process-oriented systems, in: Proceedings of the 8h ACM Symposium on Access Control Models and Technologies (SACMAT), SACMAT '03, ACM, New York, NY, USA, 2003, pp. 100–109.
[65] J. Jürjens, UMLsec: extending UML for secure systems development, Proceedings of the 5th International Conference on UML – The Unified Modeling Language, vol. 2460, Springer, 2002, pp. 412–425.
[66] M. Hafner, M. Breu, R. Breu, A. Nowak, Modelling inter-organizational workflow security in a peer-to-peer environment, in: Proceedings of the IEEE International Conference on Web Services (ICWS), 2005, pp. 533–540.
[67] M. Hafner, R. Breu, Realizing model driven security for inter-organizational workflows with WS-CDL and UML 2.0, in: Proceedings of the 8th International Conference on Model Driven Engineering Languages and Systems (MoDELS), Lecture Notes in Computer Science, vol. 3713, Springer, 2005, pp. 39–53.
[68] M. Decker, An UML profile for the modelling of mobile business processes and workflows, in: Proceedings of the 5th International Conference on Mobile Multimedia Communications (MobiMedia), ACM, Kingston upon Thames, UK, 2009, pp. 38:1–38:7.
[69] D. Domingos, A. Rito-Silva, P. Veiga, Workflow access control from a business perspective, in: Proceedings of the 6th International Conference on Enterprise Information Systems (ICEIS), vol. 3, 2004, p. 18–25.
[70] B. Mikolajczak, S. Joshi, Specifying selected security features of inter-organizational workflows, in: Proceedings of the International Conference on Computational Intelligence for Modelling, Control and Automation (CIMCA), vol. 2, IEEE Computer Society, Los Alamitos, CA, USA, 2005, pp. 958–963.

[71] H. Klarl, C. Wolff, C. Emig, Abbildung von zugriffskontrollaussagen in geschäftsprozessmodellen, in: Modellierung 2008 – Workshop Verhaltensmodellierung: Best Practices und neue Erkenntnisse, 2008, p. 14.
[72] A. Röhm, G. Pernul, G. Herrmann, Modelling secure and fair electronic commerce, in: Proceedings of the 14th Annual Computer Security Applications Conference (ACSAC), IEEE Computer Society, 1998, pp. 155–164.
[73] M. Riesner, G. Pernul, Supporting compliance through enhancing internal control systems by conceptual business process security modeling, in: Proceedings of the 21st Australasian Conference on Information Systems (ACIS), 2010, pp. 1–10.
[74] P. Herrmann, G. Herrmann, Security requirement analysis of business processes, Electronic Commerce Research 6 (2006) 305–335.
[75] G. Frankova, F. Massacci, M. Seguran, From early requirements analysis towards secure workflows, in: Proceedings of IFIPTM 2007: Joint iTrust and PST Conferences on Privacy, Trust Management and Security, Springer, 2007, pp. 407–410.
[76] J. Müller, J. Mülle, S.v. Stackelberg, K. Böhm, Secure business processes in service-oriented architectures – a requirements analysis, in: Proceedings of the 10th IEEE European Conference on Web Services (ECOWS), IEEE Computer Society, Los Alamitos, CA, USA, 2010, pp. 35–42.
[77] M. Séguran, C. Hébert, G. Frankova, Secure workflow development from early requirements analysis, in: Proceedings of the 6th European Conference on Web Services (ECOWS), IEEE Computer Society, Los Alamitos, CA, USA, 2008, pp. 125–134.
[78] N. Russell, W.M.P. van der Aalst, A. ter Hofstede, D. Edmond, Workflow resource patterns: identification, representation and tool support, in: O. Pastor, J. Falcão e Cunha (Eds.), Proceedings of the 17th International Conference on Advanced Information Systems Engineering (CAiSE), Lecture Notes in Computer Science, vol. 3520, Springer, 2005, pp. 11–42.
[79] R.S. Sandhu, E. Coyne, H. Feinstein, C. Youman, Role-based access control models, IEEE Comput. 29 (1996) 38–47.
[80] D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn, R. Chandramouli, Proposed NIST standard for role-based acces control, ACM Trans. Inform. Syst. Security 4 (2001) 224–274.
[81] E. Bertino, E. Ferrari, V. Atluri, A flexible model supporting the specification and enforcement of role-based authorization in workflow management systems, in: Proceedings of the 2nd ACM Workshop on Role-based Access Control, ACM, Fairfax, Virginia, United States, 1997, pp. 1–12.
[82] S. Oh, S. Park, Task-role-based access control model, Information Systems 28 (2003) 533–562.
[83] S. Kandala, R. Sandhu, Secure role-based workflow models, in: Proceedings of the 15th IFIP TC11/WG11.3 Annual Working Conference on Database and Application Security, vol. XV, 2002, pp. 45–58.
[84] D. Domingos, A. Rito-Silva, P. Veiga, Authorization and access control in adaptive workflows, in: Proceedings of the 8th European Symposium on Research in Computer Security (ESORICS), Springer, 2003, pp. 23–38.
[85] M. Leitner, S. Rinderle-Ma, J. Mangler, AW-RBAC: access control in adaptive workflow systems, in: Proceedings of the 6th International Conference on Availability, Reliability and Security (ARES), IEEE, 2011, pp. 27–34.
[86] R.K. Thomas, R.S. Sandhu, Towards a task-based paradigm for flexible and adaptable access control in distributed applications, in: Proceedings on the 1992–1993 Workshop on New Security Paradigms, ACM, 1993, pp. 138–142.
[87] R. Thomas, R. Sandhu, Conceptual foundations for a model of task-based authorizations, in: Proceedings of the 7th Computer Security Foundations Workshop (CSFW), 1994, pp. 66 –79.
[88] R.K. Thomas, R.S. Sandhu, Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented autorization management, in: Proceedings of the IFIP TC11 WG11.3 11th International Conference on Database Securty XI: Status and Prospects, Chapman & Hall, Ltd., 1998, pp. 166–181.
[89] V. Atluri, W.-K. Huang, Enforcing mandatory and discretionary security in workflow management systems, J. Comput. Security 5 (1997) 303–339.
[90] V. Atluri, W.-k. Huang, E. Bertino, A semantic based execution model for multilevel secure workflows, J. Comput. Security 8 (2000) 3–41.
[91] M. Kang, J. Froscher, A. Sheth, K. Kochut, J. Miller, A multilevel secure workflow management system, in: Proceedings of the 11th International Conference on Advanced Information Systems Engineering (CAISE), 1999, pp. 271–285.
[92] V. Atluri, S.A. Chun, P. Mazzoleni, Chinese wall security for decentralized workflow management systems, J. Comput. Security 12 (2004) 799–840.
[93] J. Wainer, A. Kumar, P. Barthelmess, DW-RBAC: a formal security model of delegation and revocation in workflow systems, Inform. Syst. 32 (2007) 365–384.
[94] K. Gaaloul, A. Schaad, U. Flegel, F. Charoy, A secure task delegation model for workflows, in: International Conference on Emerging Security Information, Systems, and Technologies (SECURWARE), IEEE Computer Society, Los Alamitos, CA, USA, 2008, pp. 10–15.
[95] M. Ahsant, J. Basney, Workflows in dynamic and restricted delegation, in: Proceedings of the 4th International Conference on Availability, Reliability and Security (ARES), IEEE Computer Society, 2009, pp. 17–24.
[96] K. Hasebe, M. Mabuchi, Capability-role-based delegation in workflow systems, in: Proceedings of the 8th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC), IEEE Computer Society, Los Alamitos, CA, USA, 2010, pp. 711–717.
[97] J. Crampton, H. Khambhammettu, Delegation in role-based access control, Int. J. Inform. Security 7 (2008) 123–136.
[98] M.H. Kang, J.S. Park, J.N. Froscher, Access control mechanisms for inter-organizational workflow, in: Proceedings of the sixth ACM Symposium on Access Control Models and Technologies (SACMAT), ACM, New York, NY, USA, 2001, pp. 66–74.
[99] A. Abou El Kalam, S. Benferhat, A. Miége, R.E. Baida, F. Cuppens, C. Saurel, P. Balbiani, Y. Deswarte, G. Trouessin, Organization based access control, in: Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY), IEEE Computer Society, Los Alamitos, CA, USA, 2003, pp. 120–131.
[100] S. Ayed, N. Cuppens-Boulahia, F. Cuppens, Managing access and flow control requirements in distributed workflows, in: Proceedings of the ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), IEEE Computer Society, Los Alamitos, CA, USA, 2008, pp. 702–710.
[101] M. Alam, M. Hafner, R. Breu, Constraint based role based access control in the SECTET-framework a model-driven approach, J. Comput. Security 16 (2008) 223–260.
[102] A. Schaad, K. Sohr, M. Drouineaud, A workflow-based model-checking approach to inter- and intra-analysis of organisational controls in service-oriented business processes, J. Inform. Assurance Security 2 (2007).
[103] E. Bertino, E. Ferrari, V. Atluri, The specification and enforcement of authorization constraints in workflow management systems, ACM Trans. Inform. Syst. Security 2 (1999) 65–104.
[104] M. Strembeck, J. Mendling, Generic algorithms for consistency checking of mutual-exclusion and binding constraints in a business process context, in: Proceedings of the 18th International Conference on Cooperative Information Systems (CoopIS), Lecture Notes in Computer Science, vol. 6426, Springer, 2010, pp. 204–221.
[105] R.A. Botha, J.H.P. Eloff, Separation of duties for access control enforcement in workflow environments, IBM Syst. J. 40 (2001) 666–682.
[106] F. Casati, S. Castano, M.G. Fugini, Managing workflow authorization constraints through active database technology, Inform. Syst. Front. 3 (2001) 319–338.
[107] Q. Wang, N. Li, Satisfiability and resiliency in workflow authorization systems, ACM Trans. Inform. Syst. Security (TISSEC) 13 (2010) 40:1–40:35.
[108] J. Crampton, H. Khambhammettu, Delegation and satisfiability in workflow systems, in: Proceedings of the 13th ACM Symposium on Access Control Models and Technologies (SACMAT), ACM, Estes Park, CO, USA, 2008, pp. 31–40.
[109] A. Awad, M. Weidlich, M. Weske, Specification, verification and explanation of violation for data aware compliance rules, in: Service-Oriented Computing, Lecture Notes in Computer Science, vol. 5900, Springer, 2009, pp. 500–515.
[110] S. Rinderle-Ma, J. Mangler, Integration of process constraints from heterogeneous sources in process-aware information systems, in: M. Nüttgens, O. Thomas, B. Weber (Eds.), Enterprise Modelling and Information Systems Architectures (EMISA 2011), Lecture Notes in Informatics (LNI), GI, vol. P-190, 2011, pp. 51–64.
[111] D. Knuplesch, L.T. Ly, S. Rinderle-Ma, H. Pfeifer, P. Dadam, On enabling data-aware compliance checking of business process models, in: J. Parsons, M. Saeki, P. Shoval, C. Woo, Y. Wand (Eds.), Conceptual Modeling – ER 2010, Lecture Notes in Computer Science, vol. 6412, Springer, 2010, pp. 332–346.
[112] J. Warner, V. Atluri, Inter-instance authorization constraints for secure workflow management, in: Proceedings of the 11th ACM Symposium on Access Control Models and Technologies (SACMAT), SACMAT '06, ACM, New York, NY, USA, 2006, pp. 190–199.
[113] M. Leitner, J. Mangler, S. Rinderle-Ma, Definition and enactment of instance-spanning process constraints, in: X.S. Wang, I. Cruz, A. Delis, G. Huang (Eds.), Proceedings of the 13th International Conference on Web Information Systems Engineering (WISE), Lecture Notes in Computer Science, Springer, 2012, pp. 652–658.
[114] S. Sadiq, G. Governatori, K. Namiri, Modeling control objectives for business process compliance, in: Proceedings of the 5th International Conference on Business Process Management (BPM), Lecture Notes in Computer Science, vol. 4714, Springer, 2007, pp. 149–164.
[115] L.T. Ly, S. Rinderle-Ma, K. Göser, P. Dadam, On enabling integrated process compliance with semantic constraints in process management systems – requirements, challenges, solutions, Inform. Syst. Front. 14 (2012) 195–219.
[116] S.W. Sadiq, M.E. Orlowska, W. Sadiq, Specification and validation of process constraints for flexible workflows, Inform. Syst. 30 (2005) 349–378.
[117] W.M.P. van der Aalst, Process Mining: Discovery, Conformance and Enhancement of Business Processes, Springer, 2011.
[118] L.T. Ly, S. Rinderle, P. Dadam, Integration and verification of semantic constraints in adaptive process management systems, Data Knowl. Eng. 64 (2008) 3–23.
[119] C. Ribeiro, P. Guedes, Verifying workflow processes against organization security policies, in: Proceedings of the 8th Workshop on Enabling Technologies on Infrastructure for Collaborative Enterprises (WETICE), IEEE Computer Society, 1999, pp. 190–191.
[120] K. Tan, J. Crampton, C.A. Gunter, The consistency of task-based authorization constraints in workflow systems, in: Proceedings of the 17th IEEE Workshop on Computer Security Foundations, IEEE Computer Society, 2004, p. 155.
[121] M. Kohler, A. Schaad, Avoiding policy-based deadlocks in business processes, in: Proceedings of the 3rd International Conference on Availability, Reliability and Security (ARES), IEEE Computer Society, 2008, pp. 709–716.
[122] M. Makni, S. Tata, M. Yeddes, N. Ben Hadj-Alouane, Satisfaction and coherence of deadline constraints in inter-organizational workflows, in:

Proceedings of the 18th International Conference on Cooperative Information Systems (CoopIS), Lecture Notes in Computer Science, vol. 6426, Springer, 2010, pp. 523–539.
[123] S. Schefer, M. Strembeck, J. Mendling, A. Baumgrass, Detecting and resolving conflicts of mutual-exclusion and binding constraints in a business process context, in: Proceedings of the 19th International Conference on Cooperative Information Systems (CoopIS), Lecture Notes in Computer Science (LNCS), vol. 7044, Springer, Crete, Greece, 2011, pp. 329–346.
[124] K. Barkaoui, B. Ayed, H. Boucheneb, A. Hicheur, Verification of workflow processes under multilevel security considerations, in: Proceedings of the 3rd International Conference on Risks and Security of Internet and Systems (CRiSIS), 2008, pp. 77–84.
[125] A. Schaad, V. Lotz, K. Sohr, A model-checking approach to analysing organisational controls in a loan origination process, in: Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies, SACMAT '06, ACM, New York, NY, USA, 2006, pp. 139–149.
[126] M. Barletta, S. Ranise, L. Viganó, Verifying the interplay of authorization policies and workflow in service-oriented architectures, Proceedings of the IEEE International Conference on Computational Science and Engineering (CSE), vol. 3, IEEE Computer Society, Los Alamitos, CA, USA, 2009, pp. 289–296.
[127] A. Armando, S. Ponta, Model checking of security-sensitive business processes, in: Proceedings of the 6th International Workshop on Formal Aspects in Security and Trust (FAST), Lecture Notes in Computer Science, vol. 5983, Springer, 2010, pp. 66–80.
[128] M. Pesic, W.M.P. van der Aalst, A declarative approach for flexible business processes management, in: J. Eder, S. Dustdar (Eds.), Proceedings of the Business Process Management Workshops, Lecture Notes in Computer Science, vol. 4103, Springer, 2006, pp. 169–180.
[129] M. Alberti, F. Chesani, M. Gavanelli, E. Lamma, P. Mello, M. Montali, P. Torroni, Expressing and verifying business contracts with abductive, in: G. Boella, L.v.d. Torre, H. Verhagen (Eds.), Normative Multi-agent Systems, Dagstuhl Seminar Proceedings, Internationales Begegnungs- und Forschungszentrum f++r Informatik (IBFI), Schloss Dagstuhl, Germany, Dagstuhl, Germany, 2007, pp. 1–29.
[130] M. Montali, F.M. Maggi, F. Chesani, P. Mello, W.M.P. van der Aalst, Monitoring Business Constraints with the Event Calculus, DEIS DEIS-LIA-002-11, Universita degli Studi di Bologna, 2011.
[131] A. Awad, M. Weske, Visualization of compliance violation in business process models, in: Proceedings of the Business Process Management Workshops, Lecture Notes in Business Information Processing, vol. 43, Springer, 2009, pp. 182–193.
[132] M. Weidlich, H. Ziekow, J. Mendling, O. G++nther, M. Weske, N. Desai, Event-based monitoring of process execution violations, Proceedings of the 9th International Conference on Business Process Management (BPM), vol. 6896, Springer, 2011, pp. 182–198.
[133] J. Eder, J. Mangler, E. Mussi, B. Pernici, Using stateful activities to facilitate monitoring and repair in workflow choreographies, in: Proceedings of the International Workshop on Self Healing Web Services, Congress on Services – I, 2009, pp. 219–226.
[134] F. Bezerra, J. Wainer, Anomaly detection algorithms in business process logs, in: Proceedings of the 10th International Conference on Enterprise Information Systems (ICEIS), volume AIDSS, Barcelona, Spain, 2008, p. 11–18.
[135] F. Bezerra, J. Wainer, W.M.P. van der Aalst, Anomaly detection using process mining, in: Proceedings of the 10th Workshop on Business Process Modeling, Development, and Support (BPMDS), Lecture Notes in Business Information Processing, vol. 29, Springer, 2009, pp. 149–161.
[136] W.M.P. van der Aalst, M. Dumas, C. Ouyang, A. Rozinat, E. Verbeek, Conformance checking of service behavior, ACM Trans. Internet Technol. 8 (2008) 1–30.
[137] A. Baumgrass, T. Baier, J. Mendling, M. Strembeck, Conformance checking of RBAC policies in process-aware information systems, in: Proceedings of the Business Process Management Workshops, Lecture Notes in Business Information Processing, vol. 100, Springer, 2011, pp. 435–446.
[138] R. Accorsi, C. Wonnemann, Auditing workflow executions against dataflow policies, in: Proceedings of the 13th International Conference on Business Information Systems (BIS), Lecture Notes in Business Information Processing, vol. 47, Springer, 2010, pp. 207–217.
[139] R. Accorsi, T. Stocker, On the exploitation of process mining for security audits: the conformance checking case, in: Proceedings of the 27th Annual ACM Symposium on Applied Computing (SAC), SAC '12, ACM, New York, NY, USA, 2012, pp. 1709–1716.
[140] M. Song, W.M.P. van der Aalst, Towards comprehensive support for organizational mining, Decis. Support Syst. 46 (2008) 300–317.
[141] L. Ly, S. Rinderle, P. Dadam, M. Reichert, Mining staff assignment rules from event-based data, in: Business Process Management Workshops, Lecture Notes in Computer Science, vol. 3812, Springer, 2005, pp. 177–190.
[142] M. Leitner, A. Baumgrass, S. Schefer-Wenzl, S. Rinderle-Ma, M. Strembeck, A case study on the suitability of process mining to produce current-state RBAC model, in: Proceedings of the Business Process Management Workshops, Lecture Notes in Business Information Processing, vol. 132, Springer, Tallinn, Estonia, 2012, pp. 719–724.
[143] M. Leitner, Delta analysis of role-based access control models, in: Proceedings of the 14th International Conference on Computer Aided Systems Theory (EUROCAST 2013), Lecture Notes in Computer Science, vol. 8111, Springer, 2013, pp. 507–514.
[144] F. Curbera, Y. Doganata, A. Martens, N. Mukhi, A. Slominski, Business provenance – a technology to increase traceability of end-to-end operations, in: Proceedings of the 16th International Conference on Cooperative Information Systems (CoopIS), Lecture Notes in Computer Science, vol. 5331, Springer, 2008, pp. 100–119.
[145] Y. Doganata, F. Curbera, Effect of using automated auditing tools on detecting compliance failures in unmanaged processes, in: Proceedings of the 7th International Conference on Business Process Management, Lecture Notes in Computer Science, vol. 5701, Springer, 2009, pp. 310–326.
[146] J. Eder, W. Liebhart, Workflow recovery, in: Proceedings of the 1st IFCIS International Conference on Cooperative Information Systems (CoopIS), IEEE Computer Society, Brussels, Belgium, 1996, pp. 124–134.
[147] N. Russell, W. van der Aalst, A. Hofstede, Workflow exception patterns, in: Proceedings of the 18th International Conference on Advanced Information Systems Engineering (CAiSE), Lecture Notes in Computer Science, vol. 4001, Springer, 2006, pp. 288–302.
[148] F. Casati, S. Ceri, S. Paraboschi, G. Pozzi, Specification and implementation of exceptions in workflow management systems, ACM Trans. Database Syst. (TODS) 24 (1999) 405–451.
[149] C. Hagen, G. Alonso, Exception handling in workflow management systems, IEEE Trans. Software Eng. 26 (2000) 943–958.
[150] J. Eder, M. Lehmann, Workflow data guards, in: Proceedings of the 13th International Conference on Cooperative Information Systems (CoopIS), Lecture Notes in Computer Science, vol. 3760, Springer, 2005, pp. 502–519.
[151] S. Nepal, A. Fekete, P. Greenfield, J. Jang, D. Kuo, T. Shi, A service-oriented workflow language for robust interacting applications, in: Proceedings of the 13th International Conference on Cooperative Information Systems (CoopIS), Lecture Notes in Computer Science, vol. 3760, Springer, 2005, pp. 40–58.
[152] J. Tang, S.-Y. Hwang, A scheme to specify and implement ad-hoc recovery in workflow systems, in: H.-J. Schek, G. Alonso, F. Saltor, I. Ramos (Eds.), Proceedings of the 6th International Conference on Extending Database Technology (EDBT), Lecture Notes in Computer Science, vol. 1377, Springer, 1998, pp. 484–498.
[153] R. Hamadi, B. Benatallah, Recovery nets: towards self-adaptive workflow systems, Proceedings of the 5th International Conference on Web Information Systems Engineering (WISE), vol. 3306, Springer, 2004, pp. 439–453.
[154] C. Fung, P. Hung, System recovery through dynamic regeneration of workflow specification, in: Proceedings of the 8th IEEE International Symposium on Object-Oriented Real-Time Distributed Computing (ISORC), 2005, pp. 149–156.
[155] C. Fung, P. Hung, W. Kearns, S. Uczekaj, Dynamic regeneration of workflow specification with access control requirements in MANET, in: Proceedings of the International Conference on Web Services (ICWS), 2006, pp. 761–769.
[156] M. Yu, P. Liu, W. Zang, The implementation and evaluation of a recovery system for workflows, J. Network Comput. Appl. 32 (2009) 158–183.
[157] Y. Zhu, T. Xin, I. Ray, Recovering from malicious attacks in workflow systems, in: K.V. Andersen, J. Debenham, R. Wagner (Eds.), Proceedings of the 16th International Conference on Database and Expert Systems Applications (DEXA), Lecture Notes in Computer Science, vol. 3588, Springer, 2005, pp. 14–23.
[158] I. Ray, T. Xin, Y. Zhu, Ensuring task dependencies during workflow recovery, in: F. Galindo, M. Takizawa, R. TraunMüller (Eds.), Proceedings of the 15th International Conference on Database and Expert Systems Applications (DEXA), Lecture Notes in Computer Science, vol. 3180, Springer, 2004, pp. 24–33.
[159] E. Bertino, L. Martino, F. Paci, A. Squicciarini, Security for Web Services and Service-Oriented Architectures, Springer, 2010.
[160] J. Mendling, K. Ploesser, M. Strembeck, Specifying separation of duty constraints in BPEL4People processes, in: Proceedings of the 11th International Conference on Business Information Systems (BIS), Lecture Notes in Business Information Processing, vol. 7, Springer, 2008, pp. 273–284.
[161] J. Thomas, F. Paci, E. Bertino, P. Eugster, User tasks and access control over web services, in: Proceedings of the IEEE International Conference on Web Services (ICWS), IEEE Computer Society, Los Alamitos, CA, USA, 2007, pp. 60–69.
[162] E. Bertino, J. Crampton, F. Paci, Access control and authorization constraints for WS-BPEL, in: Proceedings of the 13th IEEE International Conference on Web Services (ICWS), IEEE Computer Society, Los Alamitos, CA, USA, 2006, pp. 275–284.
[163] H. Koshutanski, F. Massacci, An access control framework for business processes for web services, in: Proceedings of the 2003 ACM workshop on XML security, XMLSEC '03, ACM, New York, NY, USA, 2003, pp. 15–24.
[164] H. Koshutanski, F. Massacci, Interactive access control for web services, in: Y. Deswarte, F. Cuppens, S. Jajodia, L. Wang (Eds.), Security and protection in information processing systems, IFIP International Federation for Information Processing, vol. 147, Springer, US, 2004, pp. 150–166.
[165] B. Carminati, E. Ferrari, P.C.K. Hung, Security conscious web service composition, in: Proceedings of the IEEE International Conference on Web Services (ICWS), IEEE Computer Society, Los Alamitos, CA, USA, 2006, pp. 489–496.
[166] C. Rudolph, N. Kuntze, Z. Velikova, Secure web service workflow execution, Electro. Notes Theor. Comput. Sci. (ENTCS) 236 (2009) 33–46.

[167] M. Altunay, D. Brown, G. Byrd, R. Dean, Trust-based secure workflow path construction, in: B. Benatallah, F. Casati, P. Traverso (Eds.), Proceedings of the 3rd International Conference on Service-Oriented Computing (ICSOC), Lecture Notes in Computer Science, vol. 3826, Springer, 2005, pp. 382–395.
[168] I. Chebbi, S. Tata, CoopFlow: a framework for inter-organizational workflow cooperation, in: Proceedings of the 13th International Conference on Cooperative Information Systems (CoopIS), Lecture Notes in Computer Science, vol. 3760, Springer, 2005, pp. 112–129.
[169] M. Hafner, R. Breu, B. Agreiter, A. Nowak, Sectet: an extensible framework for the realization of secure inter-organizational workflows, Internet Res. 16 (2006) 491–506.
[170] M. Hafner, M. Memon, R. Breu, SeAAS-A reference architecture for security services in SOA, J. Universal Comput. Sci. 15 (2009) 2916–2936.
[171] L. Lowis, R. Accorsi, Vulnerability analysis in SOA-Based business processes, IEEE Trans. Serv. Comput. 4 (2011) 230–242.
[172] M. Jensen, N. Gruschka, R. Herkenhöner, N. Luttenberger, SOA and web services: new technologies, new standards - new attacks, in: Proceedings of the 5th IEEE European Conference on Web Services (ECOWS), IEEE Computer Society, 2007, pp. 35–44.
[173] M. Jensen, N. Gruschka, R. Herkenhöner, A survey of attacks on web services, Comput. Sci. – Res. Develop. 24 (2009) 185–197.
[174] N. Gruschka, M. Jensen, N. Luttenberger, A stateful web service firewall for BPEL, in: Proceedings of the IEEE International Conference on Web Services (ICWS), Salt Lake City, UT, USA, 2007, pp. 142–149.
[175] W.-K. Huang, V. Atluri, SecureFlow: a secure web-enabled workflow management system, in: Proceedings of the 4th ACM Workshop on Role-based Access Control, ACM, Fairfax, Virginia, United States, 1999, pp. 83–94.
[176] J. Wainer, F. Bezerra, P. Barthelmess, Tucupi: a flexible workflow system based on overridable constraints, in: Proceedings of the 2004 ACM Symposium on Applied Computing, SAC '04, ACM, New York, NY, USA, 2004, pp. 498–502.
[177] C. Payne, D. Thomsen, J. Bogle, R. O'Brien, Napoleon: a recipe for workflow, in: Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC), IEEE Computer Society, Los Alamitos, CA, USA, 1999, pp. 134–142.
[178] Y. Sun, X. Meng, S. Liu, P. Pan, Flexible workflow incorporated with RBAC, in: W. Shen, K.-M. Chao, Z. Lin, J.-P. Barthŕs, A. James (Eds.), Proceedings of the 9th International Conference on Computer Supported Cooperative Work in Design II, Lecture Notes in Computer Science, vol. 3865, Springer, 2006, pp. 525–534.
[179] G. Russello, C. Dong, N. Dulay, Consent-based workflows for healthcare management, in: Proceedings of the 9th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY), IEEE Computer Society, Los Alamitos, CA, USA, 2008, pp. 153–161.
[180] G. Russello, C. Dong, N. Dulay, A workflow-based access control framework for e-health applications, in: Proceedings of the 22nd International Conference on Advanced Information Networking and Applications Workshops, IEEE Computer Society, Los Alamitos, CA, USA, 2008, pp. 111–120.
[181] P.C.K. Hung, K. Karlapalem, Secure disconnected agent interaction for electronic commerce activities using CapBasED-AMS, Information Technology and Management 3 (2002) 329–351.
[182] M. Olivier, E. Gudes, Wrappers—a mechanism to support state-based authorisation in web applications, Data Knowl. Eng. 43 (2002) 281–292.
[183] E. Gudes, A. Tubman, AutoWF: a secure web workflow system using autonomous objects, Data Knowl. Eng. 43 (2002) 1–27.
[184] D.L. Moody, Theoretical and practical issues in evaluating the quality of conceptual models: current state and future directions, Data Knowl. Eng. 55 (2005) 243–276.
[185] K.A. Scarfone, M.P. Souppaya, A. Cody, A.D. Orebaugh, SP 800-115. Technical Guide to Information Security Testing and Assessment, Technical Report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2008.
[186] S. Schefer, M. Strembeck, Modeling support for delegating roles, tasks, and duties in a process-related RBAC context, Proceedings of the Advanced Information Systems Engineering Workshops – CAiSE 2011 International Workshop, vol. 83, Springer, 2011, pp. 660–667.
[187] R. Khoury, N. Tawbi, Corrective enforcement: a new paradigm of security policy enforcement by monitors, ACM Trans. Inform. Syst. Security (TISSEC) 15 (2012) 10:1–10:27.
[188] G.L. Orgill, G.W. Romney, M.G. Bailey, P.M. Orgill, The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems, in: Proceedings of the 5th Conference on Information Technology Education, CITC5 '04, ACM, New York, NY, USA, 2004, pp. 177–181.
[189] M.E. Whitman, H.J. Mattord, Principles of Information Security, Cengage Learning, 2011.
[190] M. Leitner, M. Miller, S. Rinderle-Ma, An analysis and evaluation of security aspects in the business process model and notation, in: Proceedings of the 8th International Conference on Availability, Reliability and Security (ARES), IEEE, Regensburg, Germany, 2013, pp. 262–267.
[191] M. Leitner, S. Schefer-Wenzl, S. Rinderle-Ma, M. Strembeck, An experimental study on the design and modeling of security concepts in business processes, in: Proceedings of the 6th IFIP WG 8.1 Working Conference on the Practice of Enterprice Modeling (PoEM), Springer, Riga, Latvia, 2013, pp. 236–250.
[192] L. Fuchs, G. Pernul, R. Sandhu, Roles in information security – a survey and classification of the research area, Comput. Security 30 (2011) 748–769.
[193] W.M.P. van der Aalst, A.H.M. ter Hofstede, B. Kiepuszewski, A.P. Barros, Workflow patterns, Distribut. Parall. Databases 14 (2003) 5–51.
[194] B. Weber, M. Reichert, S. Rinderle-Ma, Change patterns and change support features – enhancing flexibility in process-aware information systems, Data Knowl. Eng. 66 (2008) 438–466.