Usage of Process Mining for Security in Process-Aware Information Systems

Marlon Müller[1]

Technical University of Munich, Munich, Germany
marlonbenedikt.mueller@tum.de

Abstract. Security in Process-Aware Information System (PAIS) is critical for almost every organisation and company, as a lack of security measures leads to vulnerabilities that can cause severe financial damage. The survey [16] by Leitner and Rinderle-Ma from 2013 analysed in a systematic literature review the researched security controls in PAIS. The authors identified that the usage of Process Mining may be an emerging topic, so this paper provides a systematic literature review to analyse the advances in Process Mining research for security in PAIS and clusters the results by the security goals that are protected as well as the Process Mining applications and concpets that can be used for security in PAIS.

Keywords: Process Mining · Security · Process-Aware Information Systems · Systematic literature review.

1 Introduction

In 2018 76% of businesses in Germany saw a significant risk for their business processes coming from cyberattacks on their information systems [5] and in a report by the Federal Bureau of Investigation from 2023 companies in the United States reported total damages of 37.5 billion US-Dollars due to cybercrime [12]. This shows the need to protect business processes from cyberattacks.
For this reason research in security for Process-Aware Information Systems (PAIS) has increased over the last years and has produced a vast amount of research papers. The survey [16] conducted a systematic literature review on security in PAIS and identified Process-Mining as an emerging technology that can be used to improve security in PAIS and predicted that the usage of Process Mining for security purposes in PAIS will be a focus of future research.
In 2018, already 65% of German businesses investigated log-files to identify security incidents based on the suspicion of a security incident and 33% used log-files to systematically identify security incidents without concrete suspicions [5].
Therefore Process Mining has the potential to be further enhanced to be used for security in Process-Aware Information Systems and was further researched in the last years. This paper aims to update the survey by Leitner and Rinderle-Ma [16] in the field of Process Mining and to provide an overview over the recent advances in the usage of Process Mining for security purposes in PAIS after 2012.

For this goal a systematic literature review will be conducted to outline the possible applications of Process Mining for security in PAIS.

To approach this goal the following research questions were targeted:

1. How does Process Mining contribute to security in PAIS?
2. Have the research challenges defined in [16] been addressed by recent research?

In Section 2 defintions and explanaitions over the terms used in this paper are provided. Section 3 evaluates related works in this field and how this paper adds further contribution to current research. Section 4 outlines the different steps of the literature review consisting of literature search, literature selection, data extraction and the classification of security goals and security concepts. The results of the literature review are described in Section 5 and in Section 6 the results are discussed and the paper is concluded.

2 Fundamentals

Below definitons for the most relevant terms in this paper are provided.

2.1 Process Mining

The main idea of Process Mining is to extract knowledge from event logs generated by existing information systems. Because event logs are often stored in an unstructured format, Process Mining uses Data Science approaches to extract the desired information in a format that can easily be analysed by humans.[1] Because Process Mining uses Data Science approaches, such as data mining or machine learning, it can be seen as the bridge between Data Science and Process Science.
Process Mining can be used for

- Process Discovery: The automatic generation of a process model based on the information extracted from an event log.
- Conformance Checking: Compare the event log of a process execution with the formal process model of that process to detect deviations.
- Enhancement: Usage of the actual process execution extracted from the event log to extend or improve an existing process model.

2.2 Information Security

Security in Information Systems (also called Information Security) is defined by the International Organization for Standardization (ISO) as the prevention of Confidentiality, Integrity and Availabilty of information [13]. This definition is also known as the CIA-Properties, but can be extended by other security goals as defined below. In other literature the term Information Security describes the

protection of systems to enter a state that allows unauthorized access to information or resources. This means, that security involves an unauthorized entity (the attacker). Security can differentiated from safety by the fact that safety describes the ability of a system to be prone to software or hardware failures from within the system itself without the influence of an attacker.[8]

Security Goals Later in this paper the results will be clustered according to the security goals that are protected by the applications proposed by the reviewed papers (Section 4 and 5.2). The clusters are chosen based on the security goals as described by Eckert in [8]. While the CIA-Properties (Confidentiality, Integrity, Availabilty) are commonly agreed on as the primary security goals the other security goals (especially Privacy and Accountability) are acknowledged as valid security goals but their relevance to different use cases is discussed and not commonly agreed on. Nonetheless this six security goals according to [8] are chosen because clustering only by the CIA-Properties would not reflect the whole bandwith of security research in Process Mining for PAIS while still allowing clear distinctions between them. The following definitions of the different security goals are taken from [8].

Confidentiality Confidentiality means to protect information from being disclosed to unauthorized entities. This includes the encryption of data as well as models to restrict the flow of information according to an organisations policies.

Integrity A system is considered to have Integrity if it provides protection against unauthorized and unnoticed manipulation of data or processes. To guarantee Integrity Access Control mechanisms are used to ensure that only authorized entities with the proper Access Rights can modify data or processes under certain constraints (e.g. limit the amount of money a user can withdraw from a bank account). In systems where manipulations can not be avoided (e.g. in network communication) cryptographic hashing should be used to detect manipulations and avoid further damages.

Availabilty Availability is the property of a system to be accessible and usable by autorized entities without unauthorized delays or restrictions. Delays that are a result of the normal operation of a system (e.g. concurrency over shared resources) are considered as authorized delays and therefore do not violate the property of Availability.

Accountability The property of Accountability (sometimes referred to as non-repudiation) is to ensure that an entity can not deny the actions it has taken. Accountability is important for Electronic Commerce to be able to prove in a lawsuit that a contract has been signed by a certain entity or that a contract has been fulfilled.

Privacy The ability of individuals to control the collection, use and disclosure of their personal information is called Privacy and obliges organisations to protect the data of identified or identifiable individuals. Privacy is considered a human right [10] and is regulated by laws like the General Data Protection Regulation (GDPR) [9] of the European Union.

Authenticity Authenticity is the valiation of the identity of an acting entity using unique identifiers or characteristics, such as cryptographic keys or biometric data. The act of verifying the identity of an entity is called authentication, that happens typically using user accounts with a distinct username and a secret password and/or biometric factors. The data that is used to verify the identity (e.g. the password) is called credentials to provide an abstraction of the concrete authentication method used.

2.3 Process-Aware Information Systems

The term Process-Aware Information Systems is definded by Dumas et al. [7] by combining the definitions of Information Systems (as PAIS are a special kind of Information Systems) and business processes. Their understanding of a business process is a "way for an organizational entity to organize work and resources (...) to accomplish its aims". On that foundation PAIS are defined as "a software system that manages and executes operational processes involving people, applications, and/or information sources on the basis of process models". Additionally to the formal defintion they marked that these process models are often represented using visual languages, like Petri-Net notations.
The main difference between a PAIS and a task-driven Information System (e.g. text editor or e-mail client) is described as the fact that task-driven applications are unaware of the process they are used in and therefore can neither support nor restrict the user in the process execution. By this differentiation PAIS are also defined as systems that support processes instead of isolated activities.[1]

3 Related Work

In this section the survey by Leitner and Rinderle-Ma [16], that this paper aims to update, is briefly summarized and other related works are presented and explained how this paper adds further contribution to the research in Process Mining for security in PAIS.

3.1 Survey by Leitner and Rinderle-Ma from 2013

The main objective of this paper is to update the systematic literature review conducted in [16] regarding the Process Mining security control and to provide an overview over the recent advances in the usage of Process Mining for security purposes in PAIS after 2012.

Summary of the survey In that survey the authors identified Process Mining as an emerging technology and gave an overview over the security related research regarding Process Mining in PAIS. The authors assigned Process Mining to the action type Detection and placed it in the Change phase of the process lifecycle.
They identified that the main usage of Process Mining for security purposes in PAIS is to examine the conformance of the process model with the actual process execution that could be derived from the event logs. The derived model from the event logs can be used to detect inconsitencies and anomalious behaviour that could be an indicator for security incidents like fraud or intrusions. Another use case the authors identified is to use event logs to validate the conformity of the process execution with the security policies of the company, like Role-Based Access Control (RBAC) models or data flow policies. It was concluded, that Process Mining can be used to capture relevant information on data, ressources and task execution to find or address security issues and compliance violations and their root causes.

Research Challenges identified For security in PAIS in general (and not only regarding Process Mining) the authors of [16] identified the research challenges that are summarized in the following part.

Agreement on Terminology and Controls The authors identified that the terminology used in the field of security in PAIS is not consistent and in some research no defintion of security or the protected security goals are provided.

Consistency with Related Fields and Concepts Even though research in security in PAIS is an interdisciplinary field, it was identified that except for the NIST standard for RBAC no standards or recommendations are considered in the research.

Measurement The authors could not identify any methods or metrics used to evaluate the effectiveness of the security controls in PAIS, while in other security areas well developed standards, e.g. the ISO/IEC 27004 standard, exist.

Testing Most of the security concepts in PAIS research are theoretical models and no method to test these models is provided.

Evaluation In the examined research the evaluation of security in PAIS centers on post-ex evaluation using Process Mining techniques and the authors stated that it should be considered how to evaluate the security in PAIS at design or run time.

Detection Controls Investigations of possible security incidents does not happen at run time but the authors identified that it could be benficial to detect anomalies at run time to be able to react to them.

Reaction Controls So far, reaction controls are focused on failure handling such as exception handling or process recovery. The authors identified that it could be beneficial to react to identified security problems at design time.

Human Orientation Human factors are not considered in the research instead it only focuses on the technological aspects of security in PAIS. The authors stressed that humans are an important factor in business processes and that they could be a security risk if they are psychologically manipulated during Social Engineering attacks.

3.2 Other Systematic Literature Reviews

The surveys [14] and [23] also conducted systematic literature reviews on the usage of Process Mining in security applications. The systematic literature review by Kelemen focused on the topics covered and the main challenges in Process Mining in the security domain [14], while the survey by Silalahi et al. identified the datasets, methods, tools and frameworks used in Process Mining research [23]. Both surveys gave a broad overview over the research in Process Mining for security applications but did not focus on security in PAIS.
This paper provides further contribution as it gives a more in depth analysis over the usage of Process Mining for security in PAIS. It also gives a unique classification of the research by identifying the security goals that are protected. As this paper narrows down the specific research field it takes a broader and more up-to-date time frame into consideration as [23] only reviewed papers between 2017 and 2021 and [14] reviewed papers between 2000 and 2016.

4 Methodology

The systematic literature review conducted in this paper follows the guidelines outlined in [4] and is also based on the methodology used in the systematic literature review by Leitner and Rinderle-Ma [16]. At first a clear definition of the research questions is given before in the second step an extensive literature search is conducted. The resulting data based on the literature search is then analysed and synthesized to answer the research questions by clustering the papers into different categories.

4.1 Research identification

This paper aims to update the survey by Leitner and Rinderle-Ma [16] in the field of Process Mining and security in PAIS and therefore to examine and evaluate the advances of security research using Process Mining in PAIS after 2012. To approach this goal the research questions formulated in Section 1 are redefined:

1. What is the contribution of security research using Process Mining in PAIS?

1.1. What security goals are protected by the applications proposed by the reviewed papers?
1.2. What Process Mining applications and concepts are used for security in PAIS?
2. How were the research challenges defined in [16] addressed by recent research?

The first research question investigates the contribution of recent research in the field of Process Mining for security in PAIS and is divided into two subquestions to give a more detailed and holistic insight into the research field. The subquestion 1.1 synthesizes the results into a classification of the security goals, as defined in Section 2.2, that are protected by the applications and methods proposed by the reviewed papers. The analysis of the Process Mining applications and concepts used for security in PAIS is done in subquestion 1.2.
To analsze how the reviewed papers contributed and addressed the research challenges presented in [16] and summarized in Section 3.1 in the second research question it is analysed what papers addressed these challenges and how they contributed to the solution of these challenges.

4.2 Literature Search

Table 1. Inclusion and Exclusion Criteria for the Literature Search and Selection

Inc 1	Search string: („process mining“ | „data mining“) & („security“ | „constraints“ | „access control“ | „authorization“) & („process aware“ | „workflow“ | „business process“)
Exc 1	The paper was published before 2013
Exc 2	The paper is not written in English
Exc 3	Title, keywords and abstract do not indicate relevance for Security, Process Mining and PAIS
Exc 4	Content is not related to the usage of Process Mining to enhance security in PAIS
Inc 2	Extend results by relevant papers from the references of the included papers

To identitfy the relevant papers for the literature review a manual search was conducted using the IEEE Xplore and Scopus databases (retrieving date: June, 17th 2024). In the literature search the search string of inclusion criteria 1 from Table 1 was used with the exclusion criteria 1 and 2 applied. Those databases were chosen because they are known for their high quality of scientific papers and their relevance to the field of Computer Science. In total 261 papers were found in the search.

4.3 Literature Selection

The results of the literature search were then filtered to reduce the amount of papers to the relevant literature for the topic of this review. The publications

Table 2. Number of papers after each step of the Literature Selection

Step No.	Applied Criteria	Number of potentially relevant Papers
1	Inc 1, Exc 1 - 2	261
2	Exc 3	38
3	Exc 4	15
4	Inc 2	17

were filtered according to the scheme in Table 2 using the inclusion and exclusion criteria from Table 1. The first step of the selection by excluding papers published before 2013 and publications not written in English was already executed during the literature search phase. In the second step of the literature review the title, keywords and abstract of the papers were reviewed to exclude papers that did not indicate to be relevant for all three topics of Process Mining, Security *and* PAIS. Because security is a broad field not all relevant papers used the term security in their title or keywords but instead used related terms like constraints, access control or authorization. This explains the inclusion of these terms in the search string and why it was necessary to review the abstracts in the second step. Because the search string was designed to result in a broad range of papers about 230 irrelevant papers were excluded during step 2, resulting in 38 remaining papers.
A detailed filtering by the content of the publications was done in the third step. If the content did not relate to the usage of Process Mining to enhance security in PAIS the paper was excluded. In this step the main challenge was to exclude papers that were related to Process Mining, security and PAIS but proposed methods that can make existing Process Mining applications more secure (e.g. by proposing secure transfer of event logs between organisations) but did not use Process Mining to enhance security in PAIS. After this step 15 papers remained for the data selection.
In the last step the references of the included papers were reviewed to find further relevant papers that might have been missed in the initial search caused by the design of the search string or because they are not indexed in the databases used for the search. The papers that were referenced by already included papers were then reviewed if they met the exclusion criteria used for the results of the initial search. In this step two additional papers were found that were referenced in [23], resulting in 17 papers for the data extraction.

4.4 Data Extraction

In the data extraxtion phase the relevant information from the publications was extracted in order to classify the publications into a meaningful and solid structure allowing to answer the research questions identified in Section 4.1. The two steps of the data extraction are illustrated in Figure 1.
In the first step the main security concept covered by the publication was identitfied. The identification of the main security concept was based on title, abstract

and keywords of the publication as well as the introduction and conclusion sections of the publication. It was assumed, that the authors would indicate the publications main security concept in these sections to give the reader a brief overview over the content of the paper and to gain their interest in the publication. For the analysis of the security concepts no automated extraction tools were used, instead the information was extracted manually. If title, abstract, keywords, introduction and conclusion indicated multiple security concepts or gave no indication of the main security concept the publication was inspected in more detail to identify the main security concept. During the categorization in security concepts it was always attempted to assign the publication to the most specific security concept possible. If this was not possible a broader security concept was chosen (e.g. Anomaly Detection is a very broad concept that could also include intrusion detection as every intrusion is also an anomaly).
In the second step the publications were classified into the security goals that are protected by the applications and methods proposed by the reviewed papers. A publication could be assigned to multiple security goals if the proposed method or application covered mutiple security goals. To classify the publications it was examined if the publication mentioned the security goals somewhere in the paper. As most of the papers did not explicitly mention the security goals, a manual classification was done by reviewing the purposes of the proposed methods and applications.
In a last step it was analysed how the reviewed papers addressed the research challenges identified in [16], for this purpose the content of the papers, especially the conclusion and discussion as well as the results sections, were reviewed and their contribution to one, or more, of the research challenges was investigated.

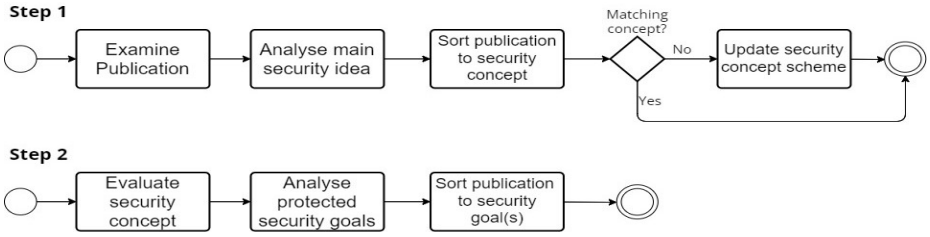

Fig. 1. Data Extraction Scheme

5 Results

This section will outline the results of the systematic literature review. At first, the publication years and publication sources of the selected publications are outlined. Secondly the contribution of Process Mining to security in PAIS based

on the reviewed literature is analysed. Lastly it is discussed how the reviewed publications addressed the research challenges that were found in [16].

5.1 Publication years and sources

Figure 2 shows the amount of papers published per year between 2013 and 2024. As the figure shows, every year 0-1 papers were published with an exception in 2013, 2020 and 2022 with respectively 3 and 4 publications. It should be noted that the results were retrieved in June 2024 and therefore the results for 2024 may not be complete. Nonetheless the figure shows that there is no clear trend visible in the amount of publications per year. As all of the publications from 2013, 2020 and 2022 were published in different sources there is no explainable reason, like a special conference or journal, for the peaks in these years.
In Table 3 the publishers of the reviewed publications are listed. It can be seen

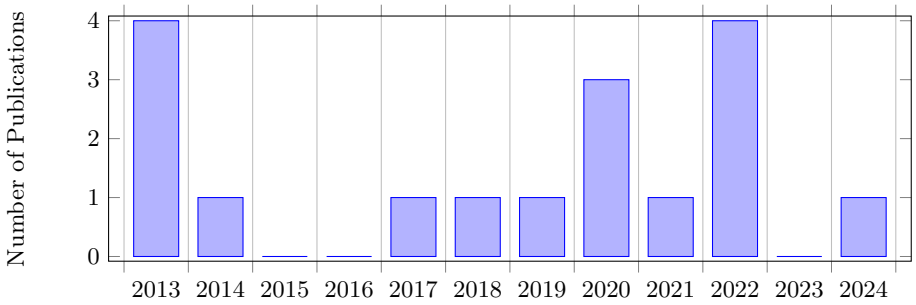

Fig. 2. Number of Publications per Year

that the majority of the publications were published by IEEE and Springer with 35% of the publications each. The other publishers have only one publication each. Table 4 lists the different sources where the papers were published. The

Table 3. Publisher of the reviewed publications

Publisher	**Publications**	**No.**
IEEE	[23], [17], [27], [19], [24], [18]	6
Springer	[3], [21], [20], [22], [26], [15]	6
Insight Society	[25]	1
Elsevier	[11]	1
IGI Global	[28]	1
ACM	[2]	1
SciTePress	[6]	1

table lists both, Journals and Venues. Only 18 % of the reviewed papers where

published in journals, the other publications where published in conference, seminar or workshop proceedings.

Table 4. Journals and Venues where the reviewed publications were published

Journal/Venue	**Publications**	**No.**
Lecture Notes in Business Information Processing	[3], [20], [15]	3
Lecture Notes in Computer Science	[21], [26]	2
International Conference on Security and Cryptography	[6]	1
International Seminar on Application for Technology of Information and Communication	[23]	1
International Journal of Advanced Science, Engineering and Information Technology	[25]	1
International Conference on Social Network Analysis, Management and Security	[17]	1
Journal of Big Data	[22]	1
Expert Systems with Applications	[11]	1
IEEE International Conference on Big Data	[27]	1
International Conference on Reliability, Infocom Technologies and Optimization	[19]	1
International Journal of Business Data Communications and Networking	[28]	1
ACM Symposium on Applied Computing	[2]	1
International Carnahan Conference on Security Technology	[24]	1
International ISC Conference on Information Security and Cryptology	[18]	1

5.2 How does Process Mining contribute to security in PAIS?

Now the concrete contributions of the reviewed papers to the field of PAIS security using Process Mining will be examined and therefore the first research question will be evaluated. In the following the papers will be clustered by the security goals that are protected by their proposed applications or methods and in the second part of this section the secruity concepts of the papers are reviewed.

Security goals The different security goals were definded in Section 2.2 and their coverage by the reviewed papers is shown in Table 5. In this table one can see that the security goals that were covered most frequently are Integrity and Confidentiality with 8 and 6 papers respectively. Because all other security goals are protected in 1 - 3 papers there is no security goal that lacks coverage totally. As described in Section 4.4 one paper could be assigned to more than one security goal, in fact if a security goal was assigned at all, only [27], [20] and [22] have only one protected security goal assigned. It should also be noted, that because of the generalistic approach of some publications it was not always

Table 5. Security goals protected by the reviewed publications

Security Goal	**Publications**	**No.**
Integrity	[15], [18], [2], [19], [21], [3], [22], [17]	8
Confidentiality	[15], [2], [19], [21], [3], [17]	6
Authenticity	[18], [2], [19], [21]	4
Privacy	[27], [20]	2
Availabilty	[19]	1
Accountability	[18]	1

possible to assign specific security goal. For instance [11] proposed a framework to detect insecure process instances, involving different kind of possible security breaches and therefore does not cover a specific security goal but offers a variety of application possibilities. In total seven papers exist that no security goal was assigned to.

Integrity The most covered security goal is Integrity with 8 papers covering this goal. Main idea of the protection of Integrity that was used in all 8 papers is the detection of unauthorized changes of data using event logs. For example, the paper [3] uses Process Mining to detect changes that were made with insufficient permissions, while [17] tries to detect and prevent the changes of authorized employees who are abusing their permissions or are manipulated by a third party.

Confidentiality While Integrity protects data from undetected, unauthorized changes, Confidentiality protects data from being accessed by unauthorized entities. As most of the papers that covered Integrity detected unauthorized actions in the event logs the papers concept can also be applied to protect the Confidentiality of the system. Only [22] and [18] just covered the detection of changes in data rather than unauthorized access in general therefore they did not cover the security goal of Confidentiality.

Availabilty Mishra et al. [19] analysed methods to detect network intrusions in PAIS using Process Mining, as network intrusions can lead to a denial of service attack this paper contributes to the security goal Availabilty.

Accountability The paper [18] tries to detect occupational fraud in business processes. In occupational fraud the employee tries to misuse the employing organizations resources for his own enrichment. Falsifying documents, like records of working hours or transaction records, is one method of occupational fraud, the detection of such falsifications is a contribution to the security goal Accountability.

Privacy In [27] Privacy is protected by assuring that an individuals Right to be Forgotten and detecting if personal data is not deleted as requested. The paper [20] focuses on the protection of privacy by detecting deviations from privacy policies caused by erroneous behaviour of employees.

Authenticity To protect the security goal of Authenticity Leitner et al. [15] used Process Mining for the derivation of Role-Based Access Control (RBAC) models while Breitmayer et al. [3], Mishra et al. [19] and Accorsi et al. [2] used Process Mining to detect unauthorized access to ressources although all of these papers used different perspectives to protect the security goal of Authenticity, as they all focused on different security concepts.

Security concepts Table 6 shows the different security concepts that were covered by the reviewed publications. In addtition to the listed publications one systematic literature review was found.

Table 6. Security concepts used in the reviewed publications

Security Concept	**Publications**	**No.**
Anomaly Detection	[11], [21], [3], [22]	4
Security Auditing	[2], [26], [25], [6]	4
GDPR Compliance	[27], [20]	2
Insider Threat Detection	[28], [17]	2
Policy Enforcement	[24]	1
Intrusion Detection	[19]	1
Fraud Detection	[18]	1
RBAC Model Derivation	[15]	1

Anomaly Detection The security concept of Anomaly Detection is a very broad concept that could subsume Intrusion Detection, Fraud Detection and Insider Threat Detection as well. Therefore papers that could not be assigned to a more specific security concept are listed under Anomaly Detection. Breitmayer et al. [3] detects the missmatch between a required permission for a task and the permission an entity actually executing it had. The other papers in this category ([11], [21], [22]) use Process Mining to detect deviations from the process model in the event logs.

Policy Enforcement The paper [24] by Talamo et al. proposed a method to detect deviations from the intended process execution and especially from security policies at runtime. Because of the runtime detection of policy violations this method allows to alert the user or administrator of the system enabling them to react and enforce the security policies in real time.

Security Auditing Under the concept of Security Auditing applications to evaluate the security properties of a system are summarized. Accorsi et al. [2] use Process Mining to discover processes and to extract structures from log files on which they can test security requirements. There are papers ([25], [6]) that use Process Mining to asses the risk (therefore possibility and potential damage) of possible security incidents.

Intrusion Detection To detect intrusions in PAIS Mishra et al. [19] use event logs to detect anomalies at run time that could indicate an intrusion of the system by monitoring the network traffic.

Fraud Detection The method to detect fraud proposed by Mardani et al. [18] is based on statistical evaluations. Process models derived from event logs were used for the evaluation and afterwards outliers in the data are detected. Their method is based on ex-post detection, because they assume that keeping flexibility at run time and beeing able to react to the fraud afterwards is more efficient than try to prevent fraud at the expense of flexibility.

Insider Threat Detection In Insider Threat Detection the focus is on the detection of malicious activities of employees or other authorised users. In [17] the authors assume that employees have a regular routine in their work, that can be analysed using Process Mining, and that sudden changes in this routine may be an indicator for malicious activities.

RBAC Model Derivation The paper [15] by Leitner et al. derives RBAC models from event logs by analysing different users and their performed actions to then derive roles and permissions from these actions.

GDPR Compliance It is no surprise that the papers [27] and [20] that covered the security goal Privacy also covered GDPR Compliance as the GDPR is one of the worlds most known privacy regulations.

5.3 Have the research challenges been addressed by recent research?

In Table 7 the research challenges that were addressed by the reviewed publications are listed. As one can see only 8 of the 17 publications adressed one (or more) of the research challenges.
Consistency with Related Fields and Concepts was addressed most frequently

Table 7. Research challenges addressed by the reviewed publications (with at least one publication addressing the challenge)

Research Challenge	**Publications**	**No.**
Consistency with Related Fields and Concepts	[27], [2], [26], [6]	4
Measurement	[6]	1
Evaluation	[26]	1
Detection Controls	[19]	1
Human Orientation	[18], [28], [17]	3

by 4 papers. Zaman et al. [27] uses standards and recommendations that evolved

based on the GDPR. Whereas the other papers ([2], [26], [6]) use state of the art Process Mining techniques for Security Auditing in PAIS.
In [6] a method to asses the security risk of a PAIS is proposed. Metrics were introduced to measure the security risk of a PAIS using numeric values, this paper therefore addresses the Measurement challenge. In contrast [26] evaluates the resilience of a PAIS during design time and is therefore addressing the Evaluation challenge.
Leitner and Rinderle-Ma [16] identified that in their literature review the research lacked detection controls at run time. Mishra et al. [19] used Process Mining to monitor network and system activities at run time to detect intrusions. This approach is a contribution to the Detection Controls challenge.
The papers [18], [28] and [17] investigate deviations in the behaviour of the systems users. This contributes to the Human Orientation challenge as they consider that humans that are involved in a process can be a security risk if they intentionally misuse the system or are victims of a social engineering attack.

6 Discussion and Conclusion

To conclude this paper in this section the main findings are summarized and limitations of this paper are discussed.

6.1 Resume

This paper reviewed recent publications that used Process Mining to enhance security in PAIS. It could be shown that every year only a few papers are published in this field, contradicting the assumption by Leitner et al. [16] that Process Mining for security in PAIS is an emerging topic. Nonetheless it was shown that the existing research in this field covers every security goal that was definded in Section 2.2. The most covered security goal is Integrity, followed by Confidentiality. Recent Process Mining research focused on a broad variety of different security concepts covering many every aspects of organisational needs for security, while the focus of the research was on post-ex Anomaly Detection and Security Auditing. Four of the research challenges identified by Leitner and Rinderle-Ma [16] were addressed by 8 of the reviewed publications, future research should evaluate if more of the research challenges can be addressed.

6.2 Limitations of this review

This paper conducted a systematic literature review including only papers centering on Process Mining, PAIS *and* security. This approach was chosen to narrow down the amount of publications and to give a more detailed insight into the research. Therefore related papers that did not focus on all three aspects may have been excluded even though they might be relevant for this topic. Another limitation is the fact that the evaluation of the addressed research challenges leaves room for interpretations so that other reviews may come to different results.

Bibliography

[1] van der Aalst, W.: Process Mining. Springer, 2nd edn. (2016), ISBN 978-3-662-49851-4, https://doi.org/10.1007/978-3-662-49851-4

[2] Accorsi, R., Stocker, T., Müller, G.: On the exploitation of process mining for security audits: The process discovery case. pp. 1462–1468 (2013), https://doi.org/10.1145/2480362.2480634, URL

[3] Breitmayer, M., Arnold, L., Reichert, M.: Permission analysis for object-centric processes. Lecture Notes in Business Information Processing **520 LNBIP**, 11–19 (2024), https://doi.org/10.1007/978-3-031-61000-4_2, URL

[4] Brereton, P., Kitchenham, B.A., Budgen, D., Turner, M., Khalil, M.: Lessons from applying the systematic literature review process within the software engineering domain. Journal of Systems and Software **80**(4), 571–583 (2007), ISSN 0164-1212, https://doi.org/https://doi.org/10.1016/j.jss.2006.07.009, URL https://www.sciencedirect.com/science/article/pii/S016412120600197X, software Performance

[5] Bundesamt für Sicherheit in der Informationstechnik: Cybersicherheits-umfrage – cyber-risiken & schutzmaßnahmen in unternehmen (Apr 2019), URL https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Cyber-Sicherheitslage-fuer-die-Wirtschaft/Cyber-Sicherheits-Umfrage/2018/2018_node.html, accessed: 2024-07-01

[6] Dedousis, P., Raptaki, M., Stergiopoulos, G., Gritzalis, D.: Towards an automated business process model risk assessment: A process mining approach. vol. 1, pp. 35–46 (2022), https://doi.org/10.5220/0011135600003283, URL

[7] Dumas, M., van der Aalst, W.M.P., ter Hofstede, A.H.M.: Process-Aware Information Systems: Bridging People and Software through Process Technology. Elsevier (2005), https://doi.org/10.1002/0471741442, URL

[8] Eckert, C.: IT-Sicherheit. De Gruyter, 10th edn. (2018), ISBN 978-3-11-055158-7

[9] European Parliament and the Council of the European Union: Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). Official Journal of the European Union **L 119** (May 2016), URL https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[10] European Union: Charter of fundamental rights of the european union. Official Journal of the European Union **55**(C 326), 391–407 (Oct 2012), ISSN 1977-091X, https://doi.org/10.3000/1977091X.C_2012.326.eng

[11] Fazzinga, B., Folino, F., Furfaro, F., Pontieri, L.: An ensemble-based approach to the security-oriented classification of low-level log traces. Expert Systems with Applications **153** (2020), https://doi.org/10.1016/j.eswa.2020.113386, URL

[12] Federal Bureau of Investigation: Internet crime report 2023 (Apr 2024)

[13] International Organization for Standardization: ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary. Geneva, 5th edn. (Feb 2018)

[14] Kelemen, R.: Systematic review on process mining and security. Central and Eastern European eDem and eGov Days **325**, 145–164 (Mar 2018), https://doi.org/10.24989/ocg.v325.13, URL https://ejournals.facultas.at/index.php/ocgcp/article/view/1542

[15] Leitner, M., Baumgrass, A., Schefer-Wenzl, S., Rinderle-Ma, S., Strembeck, M.: A case study on the suitability of process mining to produce current-state rbac models. Lecture Notes in Business Information Processing **132 LNBIP**, 719–724 (2013), https://doi.org/10.1007/978-3-642-36285-9_72, URL

[16] Leitner, M., Rinderle-Ma, S.: A systematic review on security in process-aware information systems - constitution, challenges, and future directions. Information and Software Technology **56**(3), 273–293 (2014), https://doi.org/10.1016/j.infsof.2013.12.004, cited By 58

[17] MacAk, M., Vanat, I., Merjavy, M., Jevocin, T., Buhnova, B.: Towards process mining utilization in insider threat detection from audit logs (2020), https://doi.org/10.1109/SNAMS52053.2020.9336573, URL

[18] Mardani, S., Shahriari, H.: A new method for occupational fraud detection in process aware information systems (2013), https://doi.org/10.1109/ISCISC.2013.6767348, URL

[19] Mishra, V., Dsouza, J., Elizabeth, L.: Analysis and comparison of process mining algorithms with application of process mining in intrusion detection system. pp. 613–617 (2018), https://doi.org/10.1109/ICRITO.2018.8748748, URL

[20] Mozafari Mehr, A., de Carvalho, R., van Dongen, B.: Detecting privacy, data and control-flow deviations in business processes. Lecture Notes in Business Information Processing **424 LNBIP**, 82–91 (2021), https://doi.org/10.1007/978-3-030-79108-7_10, URL

[21] Mozafari Mehr, A., M. de Carvalho, R., van Dongen, B.: An association rule mining-based framework for the discovery of anomalous behavioral patterns. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) **13725 LNAI**, 397–412 (2022), https://doi.org/10.1007/978-3-031-22064-7_29, URL

[22] Sarno, R., Sinaga, F., Sungkono, K.: Anomaly detection in business processes using process mining and fuzzy association rule learning. Journal of Big Data **7**(1) (2020), https://doi.org/10.1186/s40537-019-0277-1, URL

[23] Silalahi, S., Yuhana, U., Ahmad, T., Studiawan, H.: A survey on process mining for security. 2022 International Seminar on Application for Technology of Information and Communication: Technology 4.0 for Smart Ecosystem: A New Way of Doing Digital Business, iSemantic 2022 pp. 1–6 (2022), https://doi.org/10.1109/iSemantic55962.2022.9920473, URL

[24] Talamo, M., Arcieri, F., Schunck, C., D'Iddio, A.: Conformance checking of electronic business processes to secure distributed transactions (2013), https://doi.org/10.1109/CCST.2013.6922056, URL

[25] Yunizal, E., Santoso, J., Surendro, K.: Asset identification in information security risk assessment using process mining. International Journal on Advanced Science, Engineering and Information Technology **12**(4), 1387–1394 (2022), https://doi.org/10.18517/ijaseit.12.4.14865, URL

[26] Zahoransky, R., Koslowski, T., Accorsi, R.: Toward resilience assessment in business process architectures. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) **8696 LNCS**, 360–370 (2014), https://doi.org/10.1007/978-3-319-10557-4_39, URL

[27] Zaman, R., Cuzzocrea, A., Hassani, M.: An innovative online process mining framework for supporting incremental gdpr compliance of business processes. pp. 2982–2991 (2019), https://doi.org/10.1109/BigData47090.2019.9005705, URL

[28] Zhu, T., Guo, Y., Ju, A., Ma, J., Wang, X.: An insider threat detection method based on business process mining. International Journal of Business Data Communications and Networking **13**(2), 83–98 (2017), https://doi.org/10.4018/ijbdcn.2017070107, URL