# Usage of process mining for security in Process-Aware Information Systems

Marlon Müller

Garching bei München, July, 3rd 2024

# Recap

Until 2012 research focused on Design, Enactment and Prevention.
Detection/Evaluation was only addressed 14 times until 2012 and may be an emerging topic.

M. Leitner, S. Rinderle-Ma / Information and Software Technology 56 (2014) 273–293

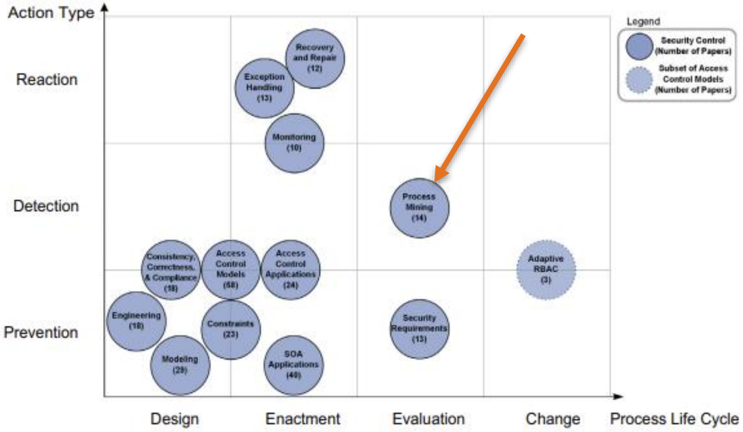


**Fig. 9.** Classification of controls.

(c) Elsevier, 2014
Source: Maria Leitner, Stefanie Rinderle-Ma:
A systematic review on security in Process-Aware Information Systems - Constitution, challenges, and future directions. Inf. Softw. Technol. 56(3): 273-293 (2014)
https://doi.org/10.1016/j.infsof.2013.12.004

# Research Questions

Q1: How does Process Mining contribute to security in PAIS?

Q2: Have the research challenges been addressed by recent research?

# Review protocol

Use IEEExplore and Scopus as resources

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 in English

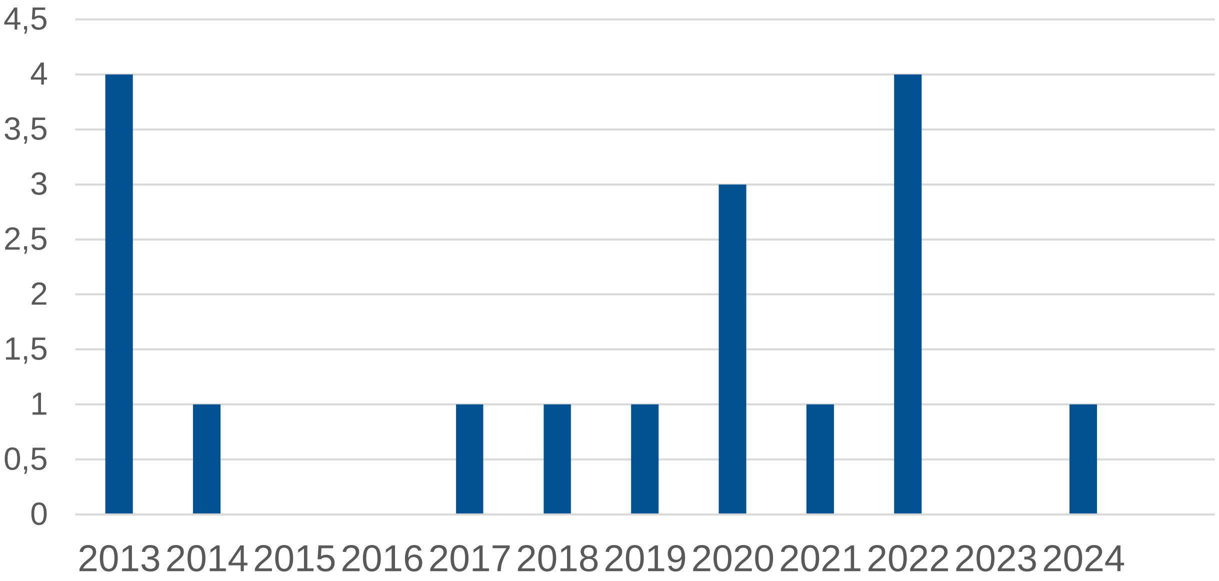
Exc 3 Title, Keywords and Abstract does not indicate relevance for Security, Process Mining and PAIS

Exc 4 Content is not related to the usage of Process Mining to enhance Security in PAIS

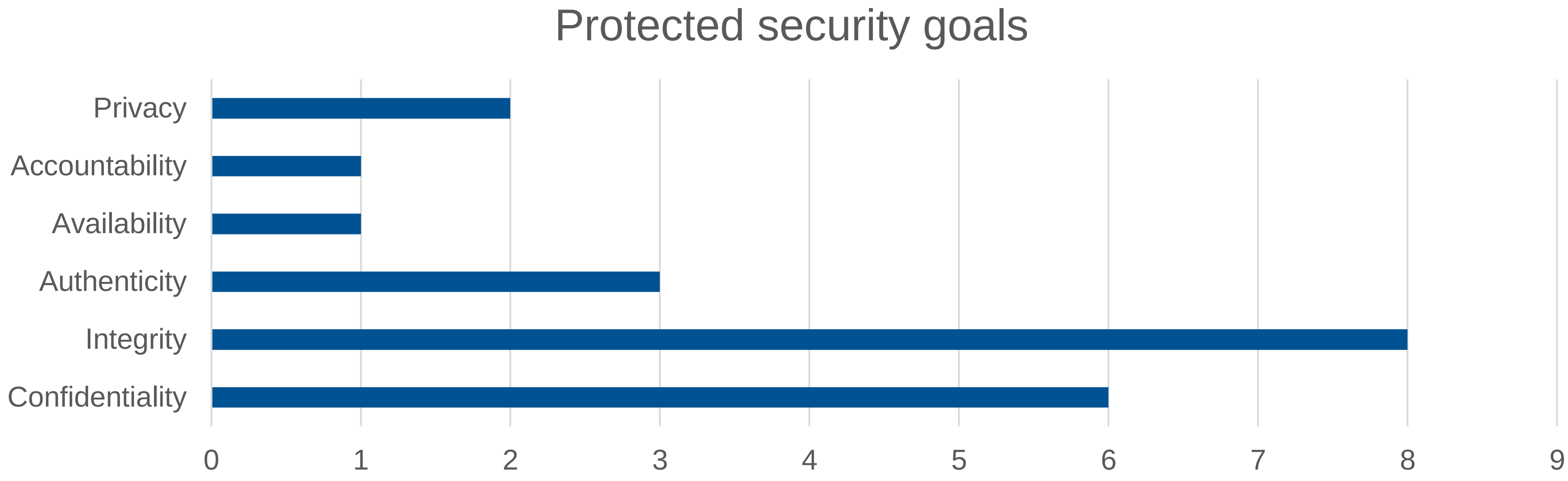
Inc 2 Extend results by relevant references

# Results

| | |
|---|---|
| Inc 1, Exc 1 - 2 | 261 |
| Exc 3 | 38 |
| Exc 4 | 15 |
| Inc 2 | 17 |

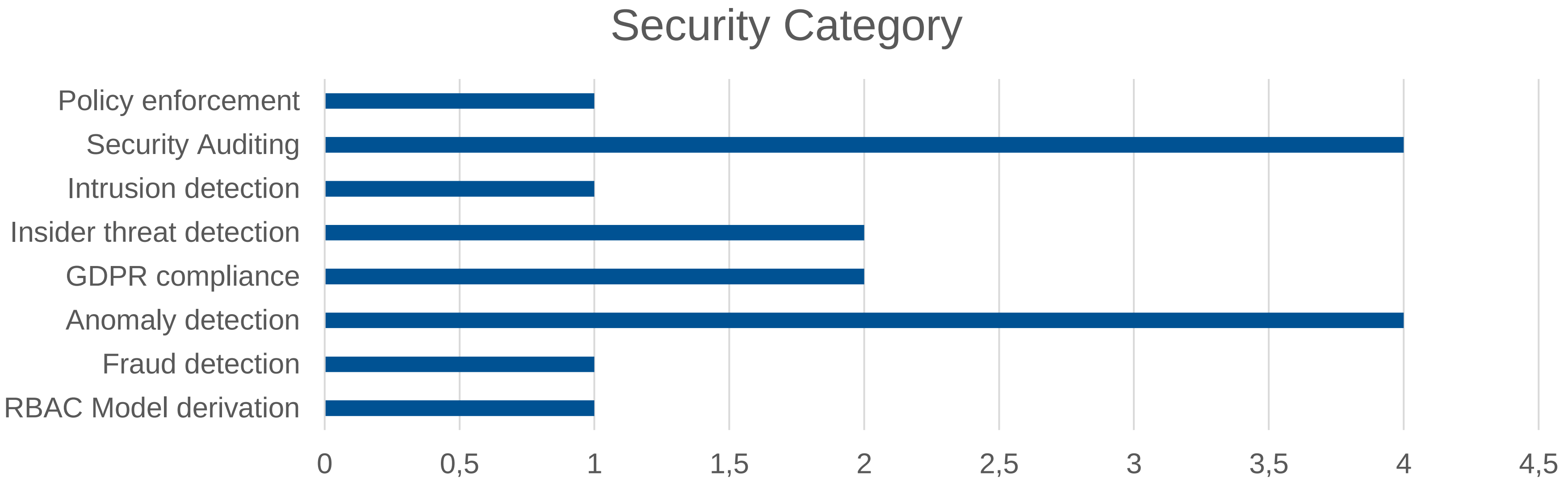


# Q1: How does Process Mining contribute to security in PAIS?



Some papers had a generalist approach and no specific security goal could be specified

# Q1: How does Process Mining contribute to security in PAIS?



Additionally, one systematic literature review was found.

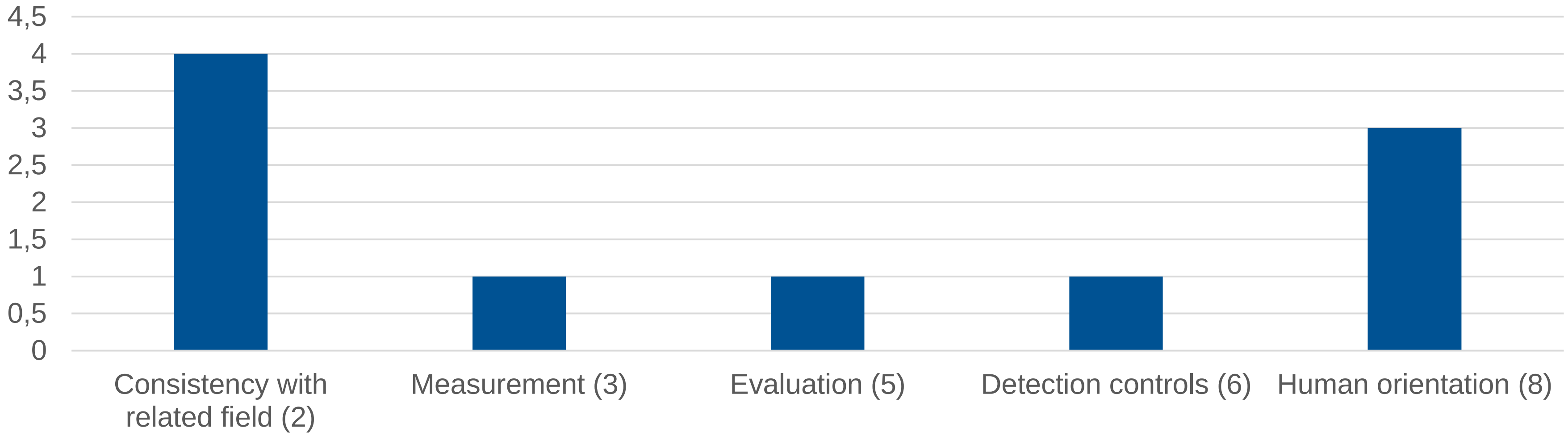
# Reminder: Challenges of security research in PAIS

1. Agreement on terminology and controls
2. Consistency with related fields and concepts
    - Take existing standards into consideration
3. Measurement
    - Adapt existing measurements and metrics into PAIS security research
4. Testing
    - Analyze which existing techniques could be adapted for PAIS
5. Evaluation
    - How can security assessment be conducted at design or run time?
6. Detection controls
    - How can intrusion detection be conducted during run time?
7. Reaction controls
    - Research should more focus on human factors and how to react to attacks
8. Human orientation
    - Humans are a big factor (social engineering), but current research focuses on technical aspects of security

# Q2: Have the research challenges been addressed?

In total only a few research challenges were addressed and not every paper addressed a research challenge.

Only 8 papers contributed to one (or more) of these challenges.



# Conclusion

The usage of Process Mining for security in PAIS was researched several times since 2013.

Research covered every security goal, while focusing on integrity.

Broad spectrum of security categories was researched, covering many aspects of operations based business process models and PAIS.

Research in this field did only slightly contribute to the original research challenges.